DOC 54 **1966/001**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

8 juli 2016

WETSONTWERP

betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties

Blz.

INHOUD

Samenvatting 3
Memorie van toelichting 4
Voorontwerp 80
Impactanalyse 110
Advies van de Raad van State 116
Wetsontwerp 143
Bijlage 179

DE SPOEDBEHANDELING WORDT DOOR DE REGERING GEVRAAGD OVEREENKOMSTIG ARTIKEL 51 VAN HET REGLEMENT.

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

8 juillet 2016

PROJET DE LOI

relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications

Pages

SOMMAIRE

Résumé 3
Exposé des motifs 4
Avant-projet 80
Analyse d'impact 113
Avis du Conseil d'État 116
Projet de loi 143
Annexe 179

LE GOUVERNEMENT DEMANDE L'URGENCE CONFORMÉMENT À L'ARTICLE 51 DU RÈGLEMENT.

De regering heeft dit wetsontwerp op 8 juli 2016 ingediend.	*Le gouvernement a déposé ce projet de loi le 8 juillet 2016.*
De "goedkeuring tot drukken" werd op 8 juli 2016 door de Kamer ontvangen.	*Le "bon à tirer" a été reçu à la Chambre le 8 juillet 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

Onderhavig ontwerp van wet beoogt de vervolmaking van het Belgisch recht met betrekking tot de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en telecommunicaties. Het opzet is meer bepaald het Wetboek van strafvordering aan te passen aan de technologische evolutie.

De voornaamste wijzigingen die door het voorontwerp worden aangebracht in het Wetboek van Strafvordering zijn:

1° verduidelijking en verbetering van het regime voor de niet-heimelijke zoeking in een informaticasysteem;

2° het uitvoeren van het cybercrime-verdrag van de Raad van Europa door de invoering van een procedure voor de bevriezing van gegevens;

3° uitbreiding van de inkijkoperatie;

4° invoering van een specifieke maatregel voor interacties of infiltraties die uitsluitend op het internet plaatsvinden

5° over het onderscheppen van telecommunicatie: samenvoeging van de heimelijke zoeking in een informaticasysteem en de onderschepping van telecommunicatie en uitbreiding van de lijst van misdrijven waarvoor de maatregel mogelijk is;

6° wettelijke basis voor een databank van stemafdrukken die in de intercepties van telecommunicaties voorkomen.

RÉSUMÉ

Le présent projet de loi vise à perfectionner le droit belge pour ce qui concerne les méthodes particulières de recherche et certaines méthodes de recherche liées à l'Internet et aux télécommunications. L'objectif est en particulier d'adapter le Code d'instruction criminelle à l'évolution technologique.

Les modifications principales apportées au Code d'instruction criminelle sont les suivantes:

1° clarification et amélioration du régime pour la recherche non secrète dans un système informatique;

2° mise en oeuvre de la convention "cybercrime" du Conseil de l'Europe par la création d'une procédure de gel des données;

3° extension du contrôle visuel discret;

4° création d'une mesure spécifique pour les interactions ou infiltrations ayant exclusivement lieu sur Internet

5° en matière d'interception des télécommunications: fusion de la recherche secrète dans un système informatique avec l'interception des télécommunications et extension de la liste des infractions pour lesquelles la mesure est possible;

6° base légale pour une banque de données des empreintes vocales qui apparaissent dans les interceptions des télécommunications.

MEMORIE VAN TOELICHTING

DAMES EN HEREN,

Inleiding

Het wetsontwerp dat aan u wordt voorgelegd bevat een aantal wijzigingen in het Wetboek van Strafvordering en het Strafwetboek en beoogt vooral een aantal verbeteringen aan te brengen in het opsporingsonderzoek en het gerechtelijk onderzoek, meer in het bijzonder in de toepassing van de bijzondere opsporingsmethoden en bepaalde andere onderzoeksmethoden die in het bijzonder betrekking hebben op de internetrecherche en elektronische en telecommunicaties.

De bepalingen die door dit voorontwerp van wet gewijzigd worden, werden door verschillende wetten ingevoerd in het Wetboek van Strafvordering. Een gemeenschappelijke eigenschap van deze wetten is dat zij gedurende geruime tijd niet hervormd of herzien zijn, met uitzondering van een aantal punctuele aanpassingen. Hieronder volgt een kort overzicht.

De wet van 6 januari 2003 betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden (B.S. 12/05/2003) voerde een wettelijke regeling in voor het gebruik van bepaalde bijzondere opsporingsmethoden. Tot dat moment werden de zogenaamde "bijzondere onderzoekstechnieken" geregeld door een vertrouwelijke ministeriële circulaire van 24 april 1990, zoals gewijzigd door de circulaire van 5 maart 1992. De belangrijkste van deze methoden zijn de observatie, de infiltratie en de informantenwerking. Daarnaast werden een aantal onderzoeksmethoden geregeld die nauw aanleunen bij de bijzondere opsporingsmethoden, maar daar als dusdanig niet onder vallen. Het ging meer bepaald om het onderscheppen van post, de inkijkoperatie, het direct afluisteren, de uitgestelde tussenkomst en het inwinnen van gegevens over bankrekeningen en banktransacties.

Een grondige hervorming van deze wet gebeurde al door de wet van 27 december 2005 houdende diverse wijzigingen van het Wetboek van Strafvordering en van het Gerechtelijk Wetboek met het oog op de verbetering van de onderzoeksmethoden in de strijd tegen het terrorisme en de zware en georganiseerde criminaliteit (B.S. 30/12/2005). Deze hervorming was grotendeels een gevolg van het arrest nr. 202/2004 van het Grondwettelijk Hof van 21 december 2004, dat een niet onaanzienlijk aantal bepalingen uit de wet van 2003 vernietigd had. Daarnaast voerde deze wet een aantal technische wijzigingen en nieuwe bepalingen in.

EXPOSÉ DES MOTIFS

MESDAMES, MESSIEURS,

Introduction

Le projet de loi qui vous est soumis contient un certain nombre de modifications apportées au Code d'instruction criminelle et au Code pénal et vise surtout à apporter un certain nombre de corrections concernant l'information et l'instruction, en particulier dans l'application des méthodes particulières de recherche et de certaines autres méthodes d'enquête spécifiques à la recherche sur Internet et aux télécommunications.

Les dispositions modifiées par le présent avant-projet de loi ont été insérées par différentes lois dans le Code d'instruction criminelle. Ces lois ont en commun de n'avoir pas été réformées ou révisées durant longtemps, hormis quelques adaptations ponctuelles. En voici un bref aperçu.

La loi du 6 janvier 2003 concernant les méthodes particulières de recherche et quelques autres méthodes d'enquête (M.B. du 12/05/2003) a introduit une réglementation légale concernant le recours à certaines méthodes particulières de recherche. Jusqu'alors, les "techniques d'enquête particulières" étaient régies par une circulaire ministérielle confidentielle du 24 avril 1990, modifiée par la circulaire du 5 mars 1992. Les principales méthodes sont l'observation, l'infiltration et le recours aux indicateurs. En outre, un certain nombre de méthodes d'enquête qui étaient étroitement liées aux méthodes particulières de recherche sans toutefois en faire partie ont été réglées. Il s'agissait plus précisément de l'interception du courrier, du contrôle visuel discret, des écoutes directes, de l'intervention différée et de la collecte de données relatives à des comptes et transactions bancaires.

Une profonde réforme de cette loi a déjà été opérée par la loi du 27 décembre 2005 portant des modifications diverses au Code d'instruction criminelle et au Code judiciaire en vue d'améliorer les modes d'investigation dans la lutte contre le terrorisme et la criminalité grave et organisée (M.B. du 30/12/2005). Cette réforme était en grande partie la conséquence de l'arrêt de la Cour constitutionnelle n° 202/2004 du 21 décembre 2004 qui avait annulé un certain nombre de dispositions de la loi de 2003. Cette loi introduisait par ailleurs un certain nombre de modifications d'ordre technique et de nouvelles dispositions.

Bij arrest nr. 105/2007 van het Grondwettelijk Hof van 19 juli 2007 werd een beperkt aantal artikelen opnieuw vernietigd. Herstelwetgeving die een antwoord bood op deze vernieting is er niet gekomen. Wel het vermelden waard is de wet van 16 januari 2009 tot wijziging van de artikelen 189*ter*, 235*ter*, 335*bis* en 416 van het Wetboek van Strafvordering. Deze wet betreft echter enkel de rechterlijke controle op de bijzondere opsporingsmethoden, en voerde verder geen nieuwe onderzoeksmogelijkheden in.

Het is dus sedert de wet van 2005 geleden dat de wetgeving over de bijzondere opsporingsmethoden een herziening onderging. Uiteraard moet daar ook noodzaak toe zijn, en de praktijk wijst uit dat deze wetgeving tot op heden goed gewerkt heeft. Het voorontwerp van wet bevat dan ook slechts een beperkt aantal bepalingen die de bijzondere opsporingsmethoden *sensu stricto* betreft. Wel is er een grondiger aanpassing van de artikelen over de inkijkoperatie, en wordt er een nieuwe bepaling ingevoerd over de interacties en infiltraties die uitsluitend op het internet gebeuren, zonder dat deze laatste daarbij onder het strikte regime van de "klassieke" infiltratie vallen.

De wet van 28 november 2000 inzake informaticacriminaliteit voerde niet alleen een aantal nieuwe misdrijven in het Strafwetboek in, maar introduceerde ook nieuwe onderzoeksmogelijkheden in het Wetboek van Strafvordering: het databeslag (artikel 39*bis*) en de netwerkzoeking (artikel 88*ter*) zijn daarvan de voornaamste. Daarnaast voerde de wet ook een medewerkingsplicht in voor personen met een bijzondere kennis van het informaticasysteem dat het voorwerp uitmaakt van de zoeking, en van diensten om gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem, te beveiligen of te versleutelen (artikel 88*quater*).

Na de ratificatie van het Verdrag van de Raad van Europa inzake informaticacriminaliteit van 23 november 2001 werd de wet van 15 mei 2006 tot wijziging van de artikelen 259*bis*, 314*bis*, 504*quater*, 550*bis* en 550*ter* van het Strafwetboek aangenomen. Deze wet was vooral een aanpassing van de strafbepalingen aan de vereisten van het Verdrag. Eigenaardig genoeg werden de bepalingen van het Wetboek van Strafvordering toen niet aangepast, hoewel het Verdrag ook bepalingen bevat over de snelle bewaring en onthulling van computergegevens, een maatregel die nog niet bestond in het Belgische recht. Dit betekent dat de onderzoeksmaatregelen in het Wetboek van Strafvordering sinds 2000 niet meer hervormd of aangepast zijn. Zestien jaar is een eeuwigheid in de snel evoluerende wereld van de informatietechnologie, en het was dan ook hoog tijd dat deze bepalingen onder

L'arrêt n° 105/2007 de la Cour constitutionnelle du 19 juillet 2007 a à nouveau annulé un nombre limité d'articles. Aucune législation réparatrice n'a apporté de réponse à cette annulation. Il est néanmoins intéressant de mentionner la loi du 16 janvier 2009 modifiant les articles 189*ter*, 235*ter*, 335*bis* et 416 du Code d'instruction criminelle. Cette loi ne porte toutefois que sur le contrôle judiciaire des méthodes particulières de recherche et n'a introduit aucune nouvelle possibilité d'investigation.

C'est donc depuis la loi de 2005 que la législation relative aux méthodes particulières de recherche a connu une révision. Évidemment, il faut qu'il y ait un besoin en ce sens et la pratique montre que jusqu'à présent cette législation a bien fonctionné. L'avant-projet de loi ne contient par conséquent qu'un nombre limité de dispositions concernant *sensu stricto* les méthodes particulières de recherche. Les articles relatifs au contrôle visuel discret ont néanmoins été adaptés en profondeur et une nouvelle disposition a été insérée concernant les interactions et infiltrations qui ont lieu exclusivement sur Internet, sans que ces dernières ne tombent sous le régime strict de l'infiltration "classique".

La loi du 28 novembre 2000 relative à la criminalité informatique a introduit non seulement un certain nombre d'infractions nouvelles dans le Code pénal mais également de nouvelles possibilités d'enquête dans le Code d'instruction criminelle: la saisie de données (article 39*bis*) et la recherche en réseau (article 88*ter*) en sont les principales. La loi a en outre introduit une obligation de collaboration pour les personnes ayant une connaissance particulière du système informatique qui fait l'objet de la recherche et les services qui permettent de protéger ou de crypter des données qui sont stockées, traitées ou transmises par un système informatique (article 88*quater*).

La loi du 15 mai 2006 modifiant les articles 259*bis*, 314*bis*, 504*quater*, 550*bis* et 550*ter* du Code pénal a été adoptée après la ratification de la Convention du Conseil de l'Europe du 23 novembre 2001 sur la cybercriminalité. Cette loi était surtout une adaptation des dispositions pénales aux exigences de la Convention. Assez curieusement, les dispositions du Code d'instruction criminelle n'avaient pas été adaptées à l'époque, bien que la Convention contienne également des dispositions sur la conservation et la divulgation rapides de données informatiques, une mesure qui n'existait pas encore en droit belge. Cela signifie que les mesures d'enquête contenues dans le Code d'instruction criminelle n'ont plus été réformées ou adaptées depuis 2000. Seize ans, c'est une éternité dans le monde de la technologie de l'information, en évolution rapide, et il était dès lors grand temps d'examiner attentivement des dispositions

de loep genomen werden met het oog op een eventuele aanpassing ervan. In het voorliggend voorontwerp van wet worden de artikelen 39*bis*, 88*ter*, en 88*quater* aangepast aan de gewijzigde noden, en worden ook de artikelen 39*ter* en 39*quater* ingevoegd, die de artikelen 16, 17, 29 en 30 van het Verdrag inzake informaticacriminaliteit omzetten in Belgisch recht.

Tot slot is er de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en openen van privécommunicatie en -telecommunicatie. Deze wet voerde de artikelen 90*ter* en volgende van het Wetboek van strafvordering in betreffende de zogenaamde "telefoontap". Hoewel deze wetgeving in het verleden al meermaals werd aangepast (onder meer door de wet van 10 juni 1998, die artikel 46*bis* invoerde), is het uitgangspunt van deze artikelen altijd ongewijzigd gebleven: de artikelen 90*ter* en volgende zijn uitsluitend van toepassing op communicatie en telecommunicatie tijdens de overbrenging ervan. De wet van 30 juni 1994 werd indertijd geschreven met uitsluitend de klassieke telefonie voor ogen, maar de realiteit is de teksten snel voorbijgehold.

Zo wordt hierbij voorbijgegaan aan de eigen realiteit van het internet, waar elektronische gegevens het voorwerp uitmaken van communicatie op de elektronische snelweg. Wat is het statuut van deze gegevens en welke is de rechtsgrond om deze gegevens in beslag te nemen of te intercepteren? Het enige kenmerkende onderscheid dat de rechtsgrond (hetzij artikel 90*ter*, hetzij artikel 88*ter*) kan bepalen, is het begrip "overbrenging" of transmissie, dat moet worden geïnterpreteerd als zijnde de overbrenging van een boodschap van verzender naar ontvanger, waarbij een bericht volgens de wetgever enkel wordt aangezien als aangekomen wanneer er een tastbaar resultaat is (bvb: bestemmeling heeft de mail gelezen).

Een uitgebreide beschrijving van de problematiek kan men terugvinden in het artikel "Internetrecherche: informaticatap en netwerkzoeking, licht aan het einde van de tunnel", door P. Van Linthout en J. Kerkhofs (T. Strafr., Kluwer, 2008, nr. 2 van april 2008, p. 79-95). De auteurs wijzen erop dat in vele gevallen onderzoeksrechters twee beschikkingen nemen: een combinatie van de netwerkzoeking (art. 88*ter*) en de informaticatap (art. 90*ter*), omdat men in de eigen realiteit van het internet nooit *a priori* kan vaststellen of bepaalde gegevens al dan niet in transmissie zijn.

Dit is een onhoudbare situatie, en het was dan ook noodzakelijk om de artikelen 90*ter* en volgende, in samenhang met de artikelen over de netwerkzoeking, te

en vue de leur adaptation éventuelle. Le présent avant-projet de loi adapte les articles 39*bis*, 88*ter* et 88*quater* à l'évolution des besoins et insère les articles 39*ter* et 39*quater*, qui transposent en droit belge les articles 16, 17, 29 et 30 de la Convention sur la cybercriminalité.

Enfin, il y a la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées. Cette loi a introduit les articles 90*ter* et suivants du Code d'instruction criminelle concernant les "écoutes téléphoniques". Bien que cette législation ait déjà été adaptée à plusieurs reprises dans le passé (notamment par la loi du 10 juin 1998 insérant l'article 46*bis*), le point de départ de ces articles est toujours resté inchangé: les articles 90*ter* et suivants s'appliquent exclusivement aux communications et télécommunications durant leur transmission. La loi du 30 juin 2014 avait été rédigée à l'époque en visant exclusivement la téléphonie classique, mais la réalité a rapidement dépassé les textes.

Ainsi, elle ignore la réalité propre de l'Internet, où les données électroniques font l'objet de communications sur les autoroutes de l'information. Quel est le statut de ces données et quel est le fondement juridique permettant de les saisir ou de les intercepter? La seule distinction caractéristique permettant de déterminer le fondement juridique (soit l'article 90*ter*, soit l'article 88tre) est la notion de "transmission", qui doit être interprétée comme la transmission d'un message de l'émetteur au récepteur, le législateur ne considérant que le message n'est arrivé à destination que s'il existe un résultat tangible (p. ex. le destinataire a lu l'e-mail).

Cette problématique est décrite en détail dans l'article "Internetrecherche: informaticatap en netwerkzoeking, licht aan het einde van de tunnel", de P. Van Linthout et J. Kerkhofs (T. Strafr., Kluwer, 2008, n° 2 d'avril 2008, p. 79-95). Les auteurs soulignent que dans de nombreux cas, les juges d'instruction rendent deux ordonnances: une combinaison de recherche en réseau (art. 88*ter*) et d'écoute informatique (art. 90*ter*) vu que dans la réalité de l'Internet il est *a priori* impossible de déterminer si certaines données sont ou non en transmission.

Cette situation est intenable et il était par conséquent nécessaire d'étudier les articles 90*ter* et suivants, conjointement aux articles relatifs à la recherche en

bestuderen met het oog op een eventuele aanpassing ervan in functie van, onder andere, de hoger geschetste problematiek.

Het hierboven kort geschetste historisch overzicht van de wetgeving omtrent de bijzondere opsporingsmethoden, de informaticacriminaliteit en de "telefoontap" toont duidelijk aan dat er verbanden zijn tussen deze drie wetgevingen die niet zomaar meer genegeerd kunnen worden. Het was dan ook de bedoeling van de regering om niet over één nacht ijs te gaan en hierover een grondig debat te kunnen voeren. De strijd tegen de georganiseerde criminaliteit en het terrorisme is er één die constant evolueert. Bij alle vormen van criminaliteit die in meer of mindere mate gerelateerd zijn aan informatietechnologie, komt steeds weer het gebrek aan effectiviteit van de opsporing en de bewijsvoering aan de orde. Naast de mogelijkheden die de informatietechnologie biedt om misdrijven te plegen, kan zij immers ook door criminelen worden aangewend om de sporen van hun activiteiten uit te wissen en als hulpmiddel om hun criminele plannen voor te bereiden en uit te voeren. Dit hangt voor een deel samen met de techniciteit van de materie en de nood aan specialisatie bij de politionele en gerechtelijke diensten. De ongrijpbaarheid van geïnformatiseerde gegevens en de snelheid waarmee dergelijke gegevens die relevant kunnen zijn voor de waarheidsvinding, verplaatst of vernietigd kunnen worden, zijn hieraan niet vreemd. Een aantal problemen vloeit echter ook voort uit het feit dat het bestaande strafprocesrecht op sommige punten niet is aangepast aan de noden van een effectieve criminaliteitsbestrijding in de informatiemaatschappij.

De nood werd gevoeld om een actualisatie door te voeren van de middelen die de gerechtelijke autoriteiten ter beschikking moeten worden gesteld om bewijzen te kunnen verzamelen in informaticasystemen. Meer en meer wordt vastgesteld dat criminelen gebruik maken van de mogelijkheden die de informatietechnologie hen biedt. Politiediensten en magistratuur dienen daarom over dezelfde middelen te beschikken. Het voorontwerp van wet wil hier dan ook een meer aangepast juridisch kader ontwerpen voor de zoeking in een informaticasysteem en het onderscheppen en kennisnemen van elektronische communicatie.

Daartoe werd binnen de FOD Justitie in april 2015 een werkgroep opgericht om hiermee aan de slag te gaan. De werkgroep was samengesteld uit vertegenwoordigers van het College van procureurs-generaal, het federaal parket, de onderzoeksrechters, de federale politie, de inlichtingendiensten, douane en accijnzen, de FOD Justitie, en het kabinet Justitie. De werkgroep kwam voor de eerste keer samen op 28 april 2015, en deed dat vanaf toen op tweewekelijkse basis.

réseau, en vue de les adapter éventuellement vis-à-vis, notamment, de la problématique dépeinte plus haut.

Le bref aperçu historique de la législation relative aux méthodes particulières de recherche, à la criminalité informatique et aux "écoutes téléphoniques", esquissé ci-dessus, établit clairement l'existence de liens tout simplement indéniables entre ces trois législations. Le gouvernement avait par conséquent pour objectif de ne pas prendre cette question à la légère et de pouvoir y consacrer un débat approfondi. La lutte contre la criminalité organisée et le terrorisme est en constante évolution. Toutes les formes de criminalité liées à des degrés différents à la technologie de l'information posent toujours la problématique du manque d'efficacité de la recherche et de l'administration de la preuve. Outre les possibilités de commettre des infractions, offertes par la technologie de l'information, celle-ci peut en effet également être utilisée par des criminels pour effacer les traces de leurs activités et comme instrument pour préparer leurs plans criminels et les mettre à exécution. C'est en partie lié à la technicité de la matière et au besoin de spécialisation dans les services policiers et judiciaires. Le caractère insaisissable des données informatisées et la rapidité avec laquelle de telles données, peut-être pertinentes pour établir la vérité, peuvent être déplacées ou détruites n'y sont pas étrangers. Toutefois, un certain nombre de problèmes découlent aussi du fait que sur certains points la procédure pénale existante n'est pas adaptée aux besoins d'une lutte effective contre la criminalité dans la société d'information.

Le besoin s'est fait sentir de procéder à une actualisation des moyens dont les autorités judiciaires doivent disposer pour pouvoir collecter des preuves dans des systèmes informatiques. Il est de plus en plus souvent constaté que les criminels recourent aux possibilités que leur offre la technologie de l'information. Les services de police et la magistrature doivent par conséquent disposer des mêmes moyens. Le présent avant-projet de loi entend dès lors créer ici un cadre juridique plus adapté pour la recherche dans un système informatique et l'interception ainsi que la prise de connaissance de communications électroniques.

En avril 2015, un groupe de travail a été constitué au sein du SPF Justice pour s'atteler à la question. Le groupe de travail se composait de représentants du Collège des procureurs généraux, du parquet fédéral, des juges d'instruction, de la police fédérale, des services de renseignement, des douanes et accises, du SPF Justice et du cabinet Justice. Il s'est réuni pour la première fois le 28 avril 2015 et a continué de le faire, depuis, sur une base bihebdomadaire.

Bij het opstellen van de teksten werd in de werkgroep steeds de noodzakelijke toets gedaan van het evenwicht tussen het belang van de waarheidsvinding enerzijds, en de rechten van de verdediging en de eerbiediging van de persoonlijke levenssfeer anderzijds. Hoe verder de gerechtelijke autoriteiten kunnen binnendringen in de persoonlijke levenssfeer van individuen, hoe groter de bescherming tegen deze indringing dient te zijn. In dat opzicht zijn belangrijke beperkingen en garanties vereist.

Het voorontwerp van wet bevat, naast grote wijzigingen, ook kleine en minder ingrijpende aanpassingen, alsook enkele aanpassingen die procedurele of administratieve vereenvoudiging tot doel hebben.

Hieronder worden nog eens de belangrijkste wijzigingen kort uiteengezet. Voor een gedetailleerde uitleg kan verwezen worden naar de artikelsgewijze bespreking.

Ten eerste wordt artikel 39*bis* Sv. het referentie-artikel op het vlak van de *niet-heimelijke* zoeking in informaticasystemen. De inhoud van artikel 88*ter* wordt hierin geïntegreerd. Er vallen vier niveaus te onderscheiden:

1° de zoeking waartoe de officier van gerechtelijke politie kan beslissen, namelijk de zoeking in een informaticasysteem dat in beslag is genomen (bekrachtiging in de wet van de rechtspraak van het Hof van Cassatie);

1° de door de procureur des Konings bevolen zoeking in een informaticasysteem dat niet in beslag is genomen maar in beslag zou kunnen worden genomen (verduidelijking van wat reeds voortvloeit uit het huidige artikel 39*bis*);

2° de door de procureur bevolen uitbreiding van een zoeking bedoeld in 1° of 2° tot een informaticasysteem dat verbonden is met het informaticasysteem dat het onderwerp is van de eerste maatregel. Die mogelijkheid, die thans is voorbehouden aan de onderzoekrechter (art. 88*ter*) maar mogelijk is in het kader van de mini-instructie, wordt overgeheveld naar art. 39*bis* en kan dus worden toegestaan door een parketmagistraat, zolang hierbij geen extra paswoorden dienen te worden gekraakt.

Tegelijk wordt de *heimelijke* zoeking in informaticasystemen ingevoerd, die is voorbehouden voor de onderzoeksrechter in het kader van het gerechtelijk onderzoek (art. 90*ter*, zie verder);

3° elke andere niet-heimelijke zoeking in een informaticasysteem. Deze soort zoeking kan enkel door een onderzoeksrechter worden bevolen.

Lors de la rédaction des textes, le groupe de travail a toujours procédé à l'indispensable examen de l'équilibre entre l'intérêt de la manifestation de la vérité d'une part et les droits de la défense ainsi que le respect de la vie privée d'autre part. Au plus les autorités judiciaires peuvent faire irruption dans la vie privée des individus, au plus grande doit être la protection contre ces intrusions. Dans cette optique, d'importantes restrictions et garanties sont requises.

L'avant-projet de loi contient, outre de grandes modifications, de petites adaptations moins radicales ainsi que quelques ajustements qui visent une simplification procédurale et administrative.

Les principales modifications sont exposées à nouveau ci-dessous. Pour une explication détaillée, il peut être renvoyé au commentaire des articles.

Premièrement, l'article 39*bis* du Code d'instruction criminelle devient l'article de référence pour ce qui regarde la recherche *non secrète* dans des systèmes informatiques. Le contenu de l'article 88*ter* y est intégré. Quatre niveaux sont à distinguer:

1° la recherche que peut ordonner la police judiciaire, à savoir la recherche dans un système informatique saisi (confirmation de la jurisprudence de la Cour de cassation dans la loi);

2° la recherche ordonnée par le procureur du roi dans un système informatique qui n'a pas été saisi mais qui pourrait l'être (clarification de ce qui découle déjà de l'actuel article 39*bis*);

3° l'extension ordonnée par le procureur d'une recherche visée au 1° ou au 2° dans un système informatique connecté au système informatique qui fait l'objet de la première mesure. Cette possibilité, actuellement réservée au juge d'instruction (art. 88*ter*) mais envisageable dans le cadre de la mini-instruction, est transférée à l'art. 39*bis* et peut donc être autorisée par un magistrat de parquet, à moins que cela n'exige pas le déchiffrement de mots de passe supplémentaires.

Dans le même temps, la recherche *en secret* dans des systèmes informatiques, réservée au juge d'instruction dans le cadre de l'instruction (art. 90*ter*, voir plus loin), est également introduite;

4° toute autre recherche non secrète dans un système informatique. Ce type de recherche ne peut être ordonné que par un juge d'instruction.

Ten tweede worden de artikelen 39*ter* en 39*quater* Sv. ingevoerd, die een procedure bevatten voor de snelle bevriezing van gegevens op verzoek van een derde staat. Deze artikelen vormen op dit vlak de uitvoering van het Cybercrimeverdrag van de Raad van Europa van 23 november 2001.

Ten derde wordt de regeling van de inkijkoperatie aangepast (artikelen 46*quinquies* en 89*ter* Sv.). Zo wordt het mogelijk gesloten voorwerpen te openen en voorwerpen mee te nemen. Ook wordt de inkijkoperatie ten aanzien van informaticasystemen mogelijk gemaakt, maar deze bevoegdheid wordt voorbehouden aan de onderzoeksrechter. Bij inkijkoperaties krijgen informaticasystemen daarmee dezelfde bescherming als de woning.

Ten vierde wordt een specifieke maatregel ingevoerd voor interacties of infiltraties die uitsluitend op internet plaatsvinden (artikel 46*sexies* Sv.). Hiervoor geldt een soepeler regime dan voor de infiltraties in de fysieke wereld, maar die soepelheid wordt gecompenseerd doordat alle contacten moeten worden geregistreerd, wat mogelijk is op internet (maar niet in de fysieke wereld).

Ten vijfde wordt de termijn voor observatie (artikel 47*sexies* Sv.), die thans één maand bedraagt maar steeds verlengbaar is, op drie maanden gebracht.

Ten zesde wordt artikel 90*ter* Sv. (m.b.t. het onderscheppen van telecommunicatie) ingrijpend hervormd:

1° introductie van de heimelijke zoeking in informaticasystemen;

1° de heimelijke zoeking in informatica-systemen en de onderschepping van telecommunicatie worden samengevoegd tot één maatregel. Door de technologische evolutie kan vaak geen onderscheid meer worden gemaakt tussen de twee;

2° de lijst van misdrijven waarvoor de maatregel van artikel 90*ter* mogelijk is (kortweg “taplijst” of “lijst 90*ter*”), wordt uitgebreid.

Ten zevende wordt een gegevensbank van stemafdrukken opgericht bij de politie om de identificatie van de verdachten te vergemakkelijken bij het afluisteren van communicatie (maatregel art. 90*ter*). Het doel is de speurders “tactische” informatie te verschaffen. Het is niet de bedoeling om juridisch bewijsmateriaal aan te leveren.

Deuxièmement, les articles 39*ter* et 39*quater* du Code d’instruction criminelle, qui renferment une procédure de gel rapide de données à la demande d’un État tiers, sont introduits. Sur ce plan, ces articles portent exécution de la Convention du Conseil de l’Europe du 23 novembre 2001 sur la cybercriminalité.

Troisièmement, la réglementation relative au contrôle visuel discret est adaptée (articles 46*quinquies* et 89*ter* du Code d’instruction criminelle). Ainsi, il devient possible d’ouvrir des objets fermés et de les emporter. Le contrôle visuel discret dans des systèmes informatiques devient également possible, cette compétence étant toutefois réservée au juge d’instruction. Dans le cadre des contrôles visuels discrets, les systèmes informatiques se voient accorder la même protection que le domicile.

Quatrièmement, une mesure spécifique est introduite pour les interactions et infiltrations qui ont lieu exclusivement sur Internet (article 46*sexies* du Code d’instruction criminelle). Un régime plus souple que pour les infiltrations dans le monde physique est appliqué, mais cette souplesse est compensée par le fait que tous les contacts doivent être enregistrés, ce qui est possible sur Internet (mais pas dans le monde physique).

Cinquièmement, le délai pour l’observation (article 47*sexies* du Code d’instruction criminelle), actuellement d’un mois mais toujours prolongeable, est porté à trois mois.

Sixièmement, l’article 90*ter* du Code d’instruction criminelle (concernant l’interception de télécommunications) est réformé en profondeur:

1° introduction de la recherche en secret dans des systèmes informatiques;

2° la recherche en secret dans des systèmes informatiques et l’interception des télécommunications sont rassemblées en une seule mesure. Du fait de l’évolution technologique, il n’est souvent plus possible de faire la distinction entre les deux;

3° la liste des infractions pour lesquelles la mesure de l’article 90*ter* est possible (en résumé, la “liste des écoutes” ou “liste 90*ter*”) est étendue.

Septièmement, une banque de données d’empreintes vocales est constituée au sein de la police afin de faciliter l’identification des suspects lors d’écoutes de communications (mesure art. 90*ter*). L’objectif est de fournir des informations “tactiques” aux enquêteurs et non d’apporter des éléments de preuve juridiques.

Alvorens over te gaan tot de artikelsgewijze bespreking, moet worden ingegaan op een algemene opmerking van de Raad van State betreffende de internationale aspecten van de informaticacriminaliteit en betreffende de territorialiteitsvraagstukken.

Het ontwerp van wet wijzigt het bestaande recht niet wat die aspecten betreft. Zoals de Raad van State aangeeft, werd in de wet inzake informaticacriminaliteit, waarbij inzonderheid artikel 39*bis* werd ingevoegd in het Wetboek van Strafvordering, reeds voorzien in enkele regels in dat verband. Zoals de Raad van State eveneens aangeeft, vloeien de wijzigingen voort uit het internationaal recht en inzonderheid uit het zogenaamde "Cybercrimeverdrag" van de Raad van Europa.

In het Wetboek van Strafvordering wordt slechts uitzonderlijk ingegaan op de territorialiteitsvraagstukken bij de omschrijving van de voorwaarden voor het gebruik van de verschillende onderzoeksmaatregelen. Die territorialiteitsvraagstukken worden immers in beginsel geregeld door het internationaal recht. Naast het "Cybercrimeverdrag" van de Raad van Europa kan bijvoorbeeld Richtlijn 2014/41/EU van 3 april 2014 betreffende het Europees onderzoeksbevel worden aangehaald, dat onder andere voorziet in een specifieke regeling voor de interceptie van telecommunicatie op grond van de plaats waar de persoon tegen wie de interceptie gericht is zich bevindt en op grond van het gegeven of de technische bijstand van de staat waar de persoon tegen wie de interceptie gericht is, al dan niet nodig is (art. 31 van richtlijn 2014/41/EU).

De territorialiteitsvraagstukken zijn bijzonder complex geworden door de ontwikkeling van de nieuwe technologieën en de sociale media.

In dit ontwerp van wet komen die territorialiteitsvraagstukken niet rechtstreeks aan bod. Overeenkomstig het arrest van het Hof van Cassatie van 18 januari 2011 (arrest Yahoo!) wordt er evenwel in verduidelijkt dat de ondernemingen die op het Belgische grondgebied een internetdienst aanbieden, moeten samenwerken met de Belgische gerechtelijke overheden in het kader van de maatregelen met het oog op de identificatie van een dienst of een abonnee (art. 46*bis* Sv.), de maatregelen met het oog op de opsporing van communicatie (art. 88*bis* Sv.) en de maatregelen met het oog op de onderschepping van communicatie of de heimelijke zoeking in een informaticasysteem (art. 90*ter* Sv.).

Parallel met de voorbereiding van het ontwerp van wet, ijveren de minister van Justitie en de Federale Overheidsdienst Justitie, in nauw overleg met de andere betrokken ministers en met de politie en het openbaar ministerie, in het bijzonder op het niveau

Avant d'entrer dans les commentaires article par article, il convient d'aborder une remarque générale du Conseil d'État sur les aspects internationaux de la criminalité informatique et sur les questions de territorialité.

Le projet de loi n'apporte pas de modification au droit existant s'agissant de ces aspects. Comme l'indique le Conseil d'État, la loi sur la criminalité informatique, qui a notamment inséré l'article 39*bis* CICr, a déjà prévu quelques règles à cet égard. Toujours comme l'indique le Conseil d'État, les changements dérivent du droit international et en particulier la convention dite "cybercrime" du Conseil de l'Europe.

Le code d'instruction criminelle n'aborde qu'exceptionnellement les questions de territorialité lorsqu'il définit les conditions d'utilisation de chaque mesure d'enquête. Ces questions de territorialité sont en effet en principe réglées par le droit international. Outre la convention "cybercrime" du Conseil de l'Europe on peut par exemple citer la Directive 2014/41/UE du 3 avril 2014 sur la décision d'enquête européenne qui prévoit par exemple un régime spécifique pour l'interception des communications suivant l'endroit où se trouve la cible de l'interception et suivant le besoin ou non de l'assistance technique de l'État où se trouve la cible (art. 31 de la directive 2014/41/UE).

Les questions de territorialité sont devenues particulièrement complexes avec le développement des nouvelles technologies et des médias sociaux.

Le présent projet de loi n'aborde pas directement ces questions de territorialité. Il précise toutefois, conformément à l'arrêt de la Cour de cassation du 18/01/2011 (arrêt Yahoo!) que les entreprises fournissant un service Internet sur le territoire belge sont tenues de coopérer avec les autorités judiciaires belges, que ce soit pour les mesures visant l'identification d'un service ou d'un abonné (art. 46*bis* CICr), celles visant le repérage des communications (art. 88*bis* CICr) et celles visant l'interception des communications ou la recherche secrète dans un système informatique (art. 90*ter* CICr).

En parallèle avec la préparation du projet de loi, le ministre et le Service public fédéral justice, en concertation étroite avec les autres ministres concernés et avec la police et le ministère public, sont actifs au niveau en particulier de l'Union européenne pour obtenir une

van de Europese Unie voor een gemeenschappelijke aanpak van de vraagstukken inzake de toegang tot elektronische gegevens in het kader van strafrechtelijke onderzoeken. Er werd een belangrijke stap gezet met de conclusies van de Raad van 9 juni 2016 over het verbeteren van de strafrechtspleging in de cyberruimte ("Council conclusions on improving criminal justice in cyberspace"). In die conclusies wordt aangegeven hoe praktische oplossingen kunnen worden verschaft en hoe deze gemeenschappelijke Europese aanpak op langere termijn kan worden ontwikkeld.

ARTIKELSGEWIJZE BESPREKING

TITEL 1

Algemene bepaling

Artikel 1

Dit artikel bepaalt de grondwettelijke basis van huidig voorontwerp van wet, met name artikel 77 van de Grondwet.

TITEL 2

Bepalingen tot wijziging van het Wetboek van strafvordering

Artikel 2

Dit artikel wijzigt artikel 39*bis* van het Wetboek van strafvordering en betreft de niet-heimelijke zoeking in informaticasystemen. Het artikel integreert de inhoud van artikel 88*ter* van het Wetboek van strafvordering betreffende de uitbreiding van een zoeking in een informaticasysteem of een deel ervan in artikel 39*bis* van hetzelfde wetboek, teneinde één coherent artikel te krijgen over de niet-heimelijke zoeking en uitbreiding daarvan in informaticasystemen. Aangezien de volledige inhoud van artikel 88*ter* wordt overgenomen, heeft dat artikel geen bestaansreden meer en wordt het opgeheven.

Daarnaast worden de bestaande bevoegdheden bij toepassing van deze zoeking verduidelijkt en uitgebreid voor wat betreft de betrokken informaticasystemen.

Artikel 88*ter* Svwerd ingevoerd door de wet van 28 november 2000 inzake informaticacriminaliteit, en is de wettelijke basis voor de zogenaamde netwerkzoeking.

Om te begrijpen in welke zin artikel 2 van het voorontwerp de mogelijkheden van de netwerkzoeking

approche commune sur ces questions de l'accès aux données électroniques dans les enquêtes pénales. Un pas important a été franchi avec les conclusions du Conseil du 9 juin 2016 sur "improving criminal justice in the cyberspace". Ces conclusions fixent la voie à suivre pour apporter des solutions pratiques mais aussi pour développer cette approche européenne commune à plus long terme.

COMMENTAIRES DES ARTICLES

TITRE 1ER

Disposition générale

Article 1er

Cet article définit la base constitutionnelle du présent avant-projet de loi, à savoir l'article 77 de la Constitution.

TITRE 2

Dispositions modifiant le Code d'instruction criminelle

Article 2

Cet article modifie l'article 39*bis* du Code d'instruction criminelle et concerne la recherche non secrète dans des systèmes informatiques. L'article intègre le contenu de l'article 88*ter* du Code d'instruction criminelle relatif à l'extension de la recherche dans un système informatique ou une partie de celui-ci dans l'article 39*bis* du même code afin d'obtenir un article cohérent sur la recherche non secrète et son extension dans des systèmes informatiques. Le contenu de l'article 88*ter* étant repris dans son intégralité, l'article n'a plus de raison d'être et est abrogé.

En outre, les compétences existantes dans le cadre de cette recherche sont clarifiées et étendues pour ce qui concerne les systèmes informatiques concernés.

L'article 88*ter* du Code d'instruction criminelle a été inséré par la loi du 28 novembre 2000 relative à la criminalité informatique et constitue le fondement légal de la recherche dans un réseau informatique.

Afin de comprendre dans quel sens article 2 de l'avant-projet de loi il étend les possibilités de recherche

uitbreidt, wordt hierna kort een overzicht gegeven van wat er momenteel al mogelijk is.

Huidige stand van het recht

Artikel 88*ter* Sv moet samen gelezen worden met de artikelen 39b*is* en 89 van het Wetboek van Strafvordering.

Op basis van artikel 39*bis* Sv. is de procureur des Konings bevoegd om een zoeking in een informaticasysteem te doen en de gegevens die erin opgeslagen zijn in beslag te nemen, er kopieën van te nemen en ze ontoegankelijk te maken (databeslag). De procureur des Konings heeft een informatieverplichting t.a.v. degene die verantwoordelijk is voor het informaticasysteem: deze wordt op de hoogte gesteld van de zoeking in het systeem en tevens wordt hem een samenvatting meegedeeld van de gegevens die zijn gekopieerd, ontoegankelijk gemaakt of verwijderd. Artikel 89 Sv. bepaalt dat de artikelen aangaande de inbeslagneming van voorwerpen door de procureur des Konings in geval van ontdekking op heterdaad, ook voor de onderzoeksrechter gelden.

Zowel de procureur des Konings als de onderzoeksrechter zijn dus op basis van artikel 39*bis* Sv. bevoegd om een zoeking in een informaticasysteem te doen. Wanneer deze zoeking echter in een woning dient te gebeuren, is de procureur des Konings slechts bevoegd in geval van ontdekking op heterdaad of indien de bewoner hierin toestemt. In alle andere gevallen is een bevel tot huiszoeking van de onderzoeksrechter vereist. Wanneer een huiszoekingsbevel is afgeleverd en er een informaticasysteem aanwezig is in de woning waarop het huiszoekingsbevel betrekking heeft, is geen afzonderlijk bevel vereist voor de zoeking in dit informaticasysteem. (*Gedr. St.*, Kamer, 1999-2000, 213/001 en 214/001, p. 20-22).

Het huidige artikel 88*ter* Sv. regelt de uitbreiding van een zoeking in een informaticasysteem. De ratio legis van artikel 88*ter* Sv. is de realiteit van de informaticawereld. Kenmerkend voor informaticasystemen – of het nu gaat om grote systemen binnen bedrijven of om handige draagbare computers – is dat ze meer en meer verbonden zijn in netwerken. Het artikel bepaalt daarom dat de zoeking in een informaticasysteem of een deel daarvan uitgebreid kan worden naar een informaticasysteem of een deel daarvan dat zich op een andere plaats bevindt dan de plaats waar de zoeking plaatsvindt. Dit volgt uit de hierboven geschetste logica van de huiszoeking: aangezien de klassieke regels van de huiszoeking bepalen dat deze enkel mag worden uitgevoerd ten aanzien van de plaats waarvoor ze wordt bevolen, en informaticasystemen meer en meer verbonden zijn in

en réseau, voici un bref aperçu de ce qu'il est déjà possible de faire actuellement.

État actuel du droit

L'article 88*ter* doit être lu conjointement avec les articles 39*bis* et 89 du Code d'instruction criminelle.

Sur la base de l'article 39*bis*, le procureur du Roi est compétent pour effectuer une recherche dans un système informatique et saisir les données qui y sont stockées, les copier et les rendre inaccessibles (saisies des données). Le procureur du Roi a un devoir d'information vis-à-vis du responsable du système informatique: celui-ci est informé de la recherche effectuée dans le système et reçoit également un résumé des données qui ont été copiées, rendues inaccessibles ou supprimées. L'article 89 du Code d'instruction criminelle précise que les articles concernant la saisie d'objets par le procureur du Roi, dans les cas de flagrant délit, s'appliquent également au juge d'instruction.

Sur la base de l'article 39*bis*, tant le procureur du Roi que le juge d'instruction sont donc compétents pour effectuer une recherche dans un système informatique. Toutefois, lorsque cette recherche doit s'effectuer dans un domicile, le procureur du Roi est uniquement compétent en cas de flagrant délit ou si l'occupant y consent. Dans tous les autres cas, un mandat de perquisition du juge d'instruction est requis. Lorsqu'un mandat de perquisition a été délivré et qu'un système informatique est présent dans le domicile qui fait l'objet du mandat de perquisition, aucun mandat distinct n'est requis pour effectuer la recherche dans ce système informatique. (*Doc. parl.*, Chambre, 1999-2000, 213/001 et 214/001, pp. 20-22).

L'actuel article 88*ter* du Code d'instruction criminelle règle l'extension d'une recherche dans un système informatique. La réalité du monde informatique constitue la ratio legis de l'article 88*ter*. Les systèmes informatiques – qu'il s'agisse de grands systèmes au sein d'entreprises ou d'ordinateurs portables compacts – se caractérisent par le fait qu'ils sont de plus en plus connectés en réseaux. C'est la raison pour laquelle l'article indique qu'une recherche dans un système informatique ou une partie de celui-ci peut être étendue à un système informatique ou à une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée. Cela découle de la logique de la perquisition esquissée ci-dessus: étant donné que les règles classiques de la perquisition prévoient que celle-ci ne peut intervenir que dans le lieu pour lequel elle a été

netwerken, zouden in principe meerdere huiszoekingsbevelen nodig zijn om de zoeking uit te breiden naar informaticasystemen op andere plaatsen. Artikel 88*ter* Sv. beoogt in de eerste plaats een oplossing te bieden voor dit probleem van de uitbreiding van een zoeking.

Artikel 88*ter*, § 1 Sv bepaalt dat voor een uitbreiding van een zoeking in een informaticasysteem enkel de onderzoeksrechter bevoegd is. Bovendien moet er aan twee cumulatieve voorwaarden voldaan zijn. Ten eerste moet deze uitbreiding noodzakelijk zijn om de waarheid aan het licht te brengen ten aanzien van het misdrijf dat het voorwerp van de zoeking uitmaakt. Uiteraard kan de uitbreiding van de zoeking niet gericht zijn op het vinden van bewijselementen met betrekking tot een misdrijf dat niet behoort tot de saisine van de onderzoeksrechter. Daarenboven is vereist dat er geen andere maatregelen voorhanden zijn die minder indringend zijn en waarmee hetzelfde resultaat kan worden bereikt of dat er een risico bestaat dat zonder deze uitbreiding bewijselementen verloren gaan.

Artikel 88*ter*, § 2 Sv preciseert dat de uitbreiding van een zoeking in een informaticasysteem zich niet verder mag uitstrekken dan tot de informaticasystemen of de delen daarvan waartoe de gebruikers van het onderzochte informaticasysteem in het bijzonder toegang hebben.

Wanneer als gevolg van de uitbreiding van de zoeking nuttige gegevens worden aangetroffen, wordt er overgegaan tot kopiename en/of ontoegankelijkmaking in overeenstemming met artikel 39*bis* Sv. De onderzoeksrechter dient dan de verantwoordelijke van het bij uitbreiding onderzochte informaticasysteem hiervan op de hoogte te brengen, tenzij diens identiteit of woonplaats redelijkerwijze niet achterhaald kan worden. Wanneer blijkt dat de na uitbreiding van de zoeking aangetroffen gegevens zich niet op het Belgische grondgebied bevinden, worden ze enkel gekopieerd. In dat geval deelt de onderzoeksrechter dit, via het openbaar ministerie, mee aan de Federale Overheidsdienst Justitie, dat dan de bevoegde overheid van de betrokken Staat hiervan op de hoogte brengt (zie artikel 88*ter*, § 3 Sv.).

Tot slot bepaalt artikel 88*ter*, § 4 Sv. dat artikel 89*bis* Sv. van toepassing is op de netwerkzoeking, m.a.w. dat deze zoeking kan opgedragen worden aan een officier van gerechtelijke politie.

Dit is de huidige stand van het recht, zoals bepaald door artikel 88*ter* van het Wetboek van Strafvordering.

ordonnée et que les systèmes informatiques sont de plus en plus souvent connectés en réseaux, plusieurs mandats de perquisition seraient en principe nécessaires pour étendre la recherche à des systèmes informatiques qui se trouvent dans d'autres lieux. L'objectif premier de l'article 88*ter* est d'apporter une solution à ce problème de l'extension d'une recherche.

L'article 88*ter*, § 1er, du Code d'instruction criminelle précise que le juge d'instruction est seul compétent pour l'extension d'une recherche dans un système informatique. Deux conditions cumulatives doivent en outre être remplies. Tout d'abord, cette extension doit être nécessaire à la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche. Il va de soi que l'extension de la recherche ne peut pas avoir pour but de trouver des éléments de preuve concernant une infraction qui ne relève pas de la saisine du juge d'instruction. Par ailleurs, il faut qu'il n'y ait pas d'autres mesures moins intrusives disponibles et permettant d'obtenir le même résultat ou qu'il existe un risque que, sans cette extension, des éléments de preuve soient perdus.

L'article 88*ter*, § 2, précise que l'extension de la recherche dans un système informatique ne peut pas excéder les systèmes informatiques ou les parties de tels systèmes auxquels ont spécifiquement accès les personnes autorisées à utiliser le système informatique qui fait l'objet de la mesure.

Si à la suite de l'extension de la recherche des données utiles sont découvertes, celles-ci sont copiées et/ou rendues inaccessibles conformément à l'article 39*bis* du Code d'instruction criminelle. Le juge d'instruction doit alors en informer le responsable du système informatique ayant fait l'objet de la recherche étendue, sauf si son identité ou son adresse ne peut être raisonnablement retrouvée. Lorsqu'il s'avère que les données recueillies par l'extension de la recherche ne se trouvent pas sur le territoire belge, elles sont seulement copiées. Dans ce cas, le juge d'instruction, par l'intermédiaire du ministère public, communique sans délai cette information au service public fédéral Justice, qui en informe les autorités compétentes de l'État concerné (voir article 88*ter*, § 3, du Code d'instruction criminelle).

Enfin, l'article 88*ter*, § 4, établit que l'article 89*bis* est applicable à la recherche en réseau, ce qui signifie que cette recherche peut être confiée à un officier de police judiciaire.

Tel est l'état actuel du droit défini à l'article 88*ter* du Code d'instruction criminelle.

Het voorontwerp van wet behoudt de huidige regeling van de zoeking en de uitbreiding van de zoeking, maar voegt er bepaalde bevoegdheden aan toe.

Ontwerp gewijzigd artikel 39*bis*

Eerst en vooral dient opgemerkt te worden dat de volgorde van de verschillende paragrafen werd gewijzigd ten opzichte van het voorontwerp dat aan de Raad van State werd voorgelegd. In eerste instantie worden de verschillende soorten zoekingen opgesomd, vervolgens wordt ingegaan op het gebruik van valse sleutels bij de verschillende soorten zoekingen, en tot slot wordt ingegaan op de gevolgen van de zoekingen (wat gebeurt er met de gegevens, informatie voor de verantwoordelijke van het informaticasysteem, en integriteit van de gegevens).

In zijn advies nr. 59 199/3 van 9 mei 2016 stelt de Raad van State de vraag of het geen aanbeveling verdient om de begrippen “informaticasysteem”, “exploitatie” en “valse sleutels” te verduidelijken (advies punt 7). Vooreerst kan er gewezen worden op het feit dat de term “exploitatie”, ingevolge punt 9 van het advies, geschrapt is uit het voorontwerp. De woorden “Onverminderd de exploitatie die voortvloeit uit de inbeslagname” in § 2, tweede lid hadden enkel tot doel de verhouding te verduidelijken tussen het eerste en het tweede lid van deze paragraaf. Het eerste lid betreft de informaticasystemen die in beslag genomen zijn, het tweede lid betreft de systemen die in beslag genomen kunnen worden. De aanhef van het tweede lid beoogt elke onzekerheid te vermijden en te verduidelijken dat het tweede lid niet begrepen mag worden alsof het de strekking van het eerste lid zou beperken. De regering meent echter dat het niet nodig is om de term “exploitatie” expliciet in het voorontwerp te behouden.

Voor het overige worden er in het voorontwerp geen definities opgenomen. Dit past niet in onze juridische traditie. Bovendien dienen de gehanteerde begrippen technologieneutraal te zijn, om te vermijden dat de concepten al te snel achterhaald zijn door de evolutie van de informatietechnologie.

Het begrip “informaticasysteem” wordt wel verduidelijkt in de memorie van toelichting bij de wet van 28 november 2000 inzake informaticacriminaliteit: met de term informaticasysteem wordt gedoeld “op alle systemen voor de opslag, verwerking of overdracht van data. Hierbij wordt vooral gedacht aan computers, chipkaarten en dergelijke, maar ook aan netwerken en delen daarvan, evenals aan telecommunicatiesystemen

L’avant-projet de loi maintient la réglementation actuelle de la recherche et de son extension mais y ajoute certaines compétences.

Article 39*bis* modifié par le projet

Il convient avant tout de faire remarquer que l’ordre des différents paragraphes a été modifié par rapport à l’avant-projet soumis à l’avis du Conseil d’État: tout d’abord, les différentes sortes de recherches sont énumérées, puis l’utilisation de fausses clés dans le cadre des différentes sortes de recherches est abordée pour terminer enfin par les incidences des recherches (qu’advient-il des données, information du responsable du système informatique et intégrité des données).

Dans son avis n° 59 199/3 du 9 mai 2016, le Conseil d’État pose la question de savoir s’il n’est pas recommandé de préciser des notions de “système informatique”, “exploitation” et “fausses clés” (point 7 de l’avis). Tout d’abord, il peut être renvoyé au fait que le terme “exploitation” a été supprimé de l’avant-projet en vertu du point 9 de l’avis. Les mots “Sans préjudice de l’exploitation découlant de la saisie” au § 2, alinéa 2, avaient pour unique objectif de clarifier le rapport entre les premier et deuxième alinéas de ce paragraphe. Le premier alinéa porte sur les systèmes informatiques saisis et le deuxième alinéa, sur les systèmes qui peuvent être saisis. Le préambule de l’alinéa 2 vise à écarter tout doute et à préciser que l’alinéa 2 ne peut être compris comme une limitation de la portée de l’alinéa 1er. Le gouvernement estime toutefois inutile de maintenir explicitement le terme “exploitation” dans l’avant-projet.

Pour le reste, l’avant-projet ne contient aucune définition. Cela n’entre pas dans le cadre de notre tradition juridique. En outre, les notions utilisées doivent être technologiquement neutres pour éviter que les concepts soient trop vite dépassés par l’évolution de la technologie de l’information.

La notion de “système informatique” est, elle, précisée dans l’exposé des motifs de la loi du 28 novembre 2000 relative à la criminalité informatique: par le terme “système informatique”, on entend “tout système permettant le stockage, le traitement ou la transmission de données. À ce propos, on pense principalement aux ordinateurs, aux cartes à puce, etc., mais également aux réseaux et à leurs composants

of onderdelen daarvan die een beroep doen op IT" (*Parl. St.* Kamer 1999-2000, nr. 0213/001, 12).

De term "valse sleutels" wordt verduidelijkt in de toelichting bij paragraaf 5.

In § 1 van artikel 39*bis*, alsook elders in het Wetboek van Strafvordering, wordt verduidelijkt dat de verschillende maatregelen die een informaticasysteem viseren, ook kunnen worden toegepast ten aanzien van een deel van een informaticasysteem.

Er wordt een nieuwe paragraaf ingevoegd, die paragraaf 2 wordt, met het oog op het verduidelijken van de bevoegdheden van de verschillende actoren op het vlak van zoeking in een informaticasysteem. Het huidige artikel 39*bis* is in dat opzicht immers niet duidelijk genoeg. Er is voorzien in een systeem met vier niveaus.

Paragraaf 2, eerste lid: Het eerste niveau is dat van de zoeking in een informaticasysteem dat in beslag werd genomen in het kader van het onderzoek. Die zoeking kan worden uitgevoerd door de officier van gerechtelijke politie zonder voorafgaande machtiging van de procureur des Konings of van de onderzoeksrechter. In zijn arrest van 11 februari 2015 (AR P.14 1739.F) stelde het Hof van Cassatie immers dat het huidige recht de officier van gerechtelijke politie reeds toestaat om kennis te nemen van de gegevens die zijn opgeslagen in een in beslag genomen gsm. Uiteraard gebeurt de exploitatie van de gegevens steeds binnen de grenzen van het strafrechtelijk onderzoek en onder controle van de magistraat die ermee is belast.

Concrete voorbeelden:

— De politie betrapt een drugdealer op heterdaad met op zak één (en vaak meerdere) gsm's/smartphones. De dealer wordt gearresteerd en de toestellen worden inbeslaggenomen. De politie zal deze toestellen kunnen uitlezen indien dit nuttig is voor het onderzoek, zelfs zonder vordering daartoe van een magistraat. Vaak gebeurt het dat hierop berichten worden aangetroffen van bv. bestellingen van drugs, afspraken voor leveringen, contacten met afnemers of bovendealers…

— Tijdens een actie tegen rondtrekkende dadergroepen verantwoordelijk voor nachtelijke inbraken, wordt in een residentiële woonwijk een verdacht voertuig met drie inzittenden aangetroffen; bij verder onderzoek treft men inbraakmateriaal, smartphones, gps-toestel aan. Bij verder onderzoek zal de politie deze toestellen kunnen exploiteren (het is bijvoorbeeld al regelmatig gebeurd dat bij het aantreffen van een gps-toestel aan de hand van ingegeven adressen de verdachten kunnen gelinkt

ainsi qu'aux systèmes de télécommunication ou à leurs composants qui font appel à la technologie de l'information" (*Doc. parl.*, Chambre, 1999-2000, n° 213/001, 12).

Le terme "fausses clés" est expliqué au paragraphe 5 de l'exposé des motifs.

Au § 1er de l'article 39*bis*, ainsi qu'ailleurs dans le Code d'instruction criminelle, il est précisé que les diverses mesures qui visent un système informatique peuvent également être appliquées à l'égard d'une partie d'un système informatique.

Un nouveau paragraphe est inséré, qui devient le paragraphe 2, pour clarifier quelles sont les compétences des différents acteurs en matière de recherche dans un système informatique. L'article 39*bis* actuel manque en effet de clarté à cet égard. Un régime à quatre niveaux est prévu.

Paragraphe 2, alinea 1: Le premier niveau est celui de la recherche dans un système informatique qui a été saisi dans le cadre de l'enquête. Cette recherche peut être exécutée par l'officier de police judiciaire sans autorisation préalable du procureur du Roi ou du juge d'instruction. Dans son arrêt du 11 février 2015 (AR P.14 1739.F), la Cour de cassation a en effet indiqué que le droit actuel permet déjà à l'officier de police judiciaire de prendre connaissance des données d'un GSM qui a été saisi. Bien entendu, l'exploitation des données se déroule toujours dans les limites de l'enquête pénale et sous le contrôle du magistrat en charge de celle-ci.

Exemples concrets:

— La police attrape en flagrant délit un revendeur de drogue ayant en poche un (et souvent plusieurs) gsm/smartphone(s). Le dealer est arrêté est les appareils sont saisis. La police pourra lire ces appareils, si cela est utile pour l'enquête, même en l'absence de réquisition d'un magistrat. Souvent, on y trouvera des messages concernant, par exemple, des commandes de drogue, des arrangements pour la livraison, des contacts avec des clients ou de plus gros dealers, etc.

— Au cours d'une action contre des bandes itinérantes responsables de cambriolages la nuit, un véhicule suspect avec trois occupants est repéré dans un quartier résidentiel; en approfondissant la recherche, on découvre du matériel facilitant l'effraction, des smartphones, un appareil gps. Par la suite, la police pourra exploiter ces appareils (à titre d'exemple, il est déjà régulièrement arrivé lorsqu'un appareil gps est trouvé que des suspects puissent être liés à d'autres

worden aan andere feiten, of nog dat aan de hand van het ingegeven thuisadres kan vastgesteld worden dat het toestel afkomstig is uit een inbraak en de benadeelde kon gevonden worden).

— Bij een huiszoeking worden verschillende computers en geheugenkaarten inbeslaggenomen (laptops, desktop, notebooks, USB-sticks …): deze kunnen vervolgens onderzocht door de gespecialiseerde computer crime units van de (federale) politie: hiervoor is niet telkens een bevel nog van de procureur des Konings nodig.

Paragraaf 2, tweede lid: het tweede niveau betreft de zoeking in een informaticasysteem dat niet in beslag is genomen maar waarvoor alle wettelijke voorwaarden voor een inbeslagneming zijn vervuld. Met andere woorden: er bestaat een juridische mogelijkheid om het informaticasysteem in beslag te nemen, maar om bepaalde redenen acht men dit niet wenselijk of noodzakelijk. In dat geval moet de procureur des Konings machtiging verlenen voor de zoeking. Dat vloeit reeds voort uit het huidige artikel 39*bis*, § 2.

Voorbeelden:

— De onderzoekers volgen een persoon die het onderwerp is van een onderzoek voor deelname aan een terroristische groep. De persoon brengt enige tijd door in een cybercafé. De onderzoekers wensen de computer te onderzoeken die de persoon heeft gebruikt. De procureur des Konings zou kunnen beslissen om de computer in beslag te nemen, maar die inbeslagneming is niet onontbeerlijk omdat het enkel de bedoeling is te weten te komen welke sites de persoon heeft geraadpleegd. In dat geval kan de procureur des Konings de onderzoekers machtigen om een zoeking uit te voeren in de computer.

— In het kader van een belangrijk financieel onderzoek moeten de onderzoekers een zoeking doen in het informaticasysteem van een bank. De inbeslagneming van het informaticasysteem is mogelijk maar kan de betrokken bank zware werkingsmoeilijkheden berokkenen. Het parket kan er in dat geval de voorkeur aan geven om de onderzoekers opdracht te geven de zoeking in het informaticasysteem uit te voeren zonder over te gaan tot de inbeslagneming.

Paragraaf 2, derde lid verduidelijkt op vraag van de Raad van State dat enkel het informaticasysteem in kwestie geëxploiteerd mag worden.

Teneinde te vermijden dat bv. de volledige Dropbox-account, die toegankelijk is vanaf een smartphone, wordt geëxploiteerd, zal elke externe verbinding die het toestel maakt (gsm-verbinding, wifi-connectie…)

faits grâce aux adresses encodées dans l'appareil, ou qu'on puisse constater grâce à l'adresse encodée du domicile que l'appareil provient d'un cambriolage et la personne lésée a pu être retrouvée).

— Lors d'une perquisition, différents ordinateurs et cartes mémoire sont saisis (laptops, desktops, notebooks, sticks USB, etc.): ils pourront ensuite être exploités par les computer crime units spécialisées de la police (fédérale): un mandat du procureur du Roi n'est pas systématiquement nécessaire pour ce faire.

Paragraphe 2, alinéa 2: le deuxième niveau concerne la recherche dans un système informatique qui n'a pas été saisi, mais pour lequel toutes les conditions légales d'une saisie sont réunies. En d'autres termes, il existe une possibilité juridique de saisir le système informatique, mais, pour certaines raisons, cette saisie est considérée comme non souhaitable ou non nécessaire. Dans ce cas, la recherche doit être autorisée par le procureur du Roi. Ceci découle déjà de l'article 39*bis* § 2 actuel.

Exemples:

— Les enquêteurs suivent une personne faisant l'objet d'une enquête pour participation à un groupe terroriste. La personne passe quelque temps dans un cybercafé. Les enquêteurs souhaitent analyser l'ordinateur qui a été utilisé par la personne. Le procureur du Roi pourrait décider la saisie de l'ordinateur mais cette saisie n'est pas indispensable car il s'agit seulement de savoir quels sites ont été consultés par la personne. Dans ce cas, le procureur du Roi pourra autoriser les enquêteurs à faire la recherche dans l'ordinateur.

— Dans le cadre d'une enquête financière importante, les enquêteurs doivent faire une recherche dans le système informatique d'une banque. La saisie du système informatique est possible mais peut causer des difficultés importantes de fonctionnement à la banque en question. Le parquet pourra dans ce cas préférer charger les enquêteurs de faire la recherche dans le système informatique sans procéder à la saisie.

Le paragraphe 2, alinéa 3, précise, à la demande du Conseil d'État, que seul le système informatique en question peut être exploité.

Afin d'éviter par exemple que le compte Dropbox complet accessible à partir d'un smartphone soit exploité, les services de police couperont chaque liaison externe établie par l'appareil (liaison gsm, connexion

door de politiediensten uitgezet worden, bijvoorbeeld door de vliegtuigstand in te schakelen of het toestel te exploiteren in een “Faraday-omgeving”. Op deze wijze is men er zeker van dat enkel de gegevens die op het toestel zelf opgeslagen zijn, geëxploiteerd worden.

In punt 10 van zijn advies vraagt de Raad van State of het feit dat elke externe verbinding door de politiediensten dient te worden uitgeschakeld niet moet worden opgenomen in de tekst zelf van het ontwerp. De regering acht het nuttig om hierop in te gaan en heeft dus een derde lid toegevoegd aan § 2 waarin gesteld wordt dat de zoekingen bedoeld in deze paragraaf zich enkel kunnen uitstrekken tot de gegevens die opgeslagen zijn op het al dan niet in beslag genomen informaticasysteem.

Op basis van deze redenering mogen politieambtenaren, indien ze alle externe verbindingen van het informaticasysteem hebben uitgeschakeld, zonder machtiging van een magistraat ook *apps* openen die op dit systeem zijn geïnstalleerd. Ze mogen bijvoorbeeld de Facebook-app, mailing-apps (zoals Hotmail, Gmail etc.) en messenger-apps (zoals Whatsapp, Viber etc.) openen en de gegevens, waaronder e-mails en tekstberichten, uitlezen. Deze gegevens bevinden zich namelijk noodzakelijkerwijze op het toestel zelf, waardoor ze geëxploiteerd mogen worden.

In punt 6 van zijn advies zegt de Raad van State dat het niet duidelijk is waarom in artikel 39*bis* gewag gemaakt wordt van zowel de procureur des Konings als de arbeidsauditeur, terwijl dit in de rest van het ontwerp niet langer het geval is. Het woord “arbeidsauditeur” werd in artikel 39*bis* en in artikel 88*quater* ingevoegd door de wet van 6 juni 2010 tot invoering van het Sociaal Strafwetboek. De memorie van toelichting bij deze wet verduidelijkt dat hierdoor “de arbeidsauditeur dezelfde bevoegdheden heeft als de procureur des Konings. De sociaal inspecteurs kunnen in de hoedanigheid van officier van gerechtelijke politie het openbaar ministerie bijstaan bij een strafrechtelijk onderzoek ter bestrijding van informaticacriminaliteit” (*Parl.St.* Kamer 2008-2009, nr. 52-1666/001, 324).

De regering is het eens met de Raad van State dat dit verwarring schept. Men zou immers *a contrario* kunnen redeneren dat de arbeidsauditeur geen andere bevoegdheden heeft, of dat artikel 39*bis* zou kunnen toegepast worden met uitsluiting van de federale procureur of de procureur-generaal. Gelet op artikel 22 van het Wetboek van strafvordering en de artikelen 152 en 155 van het Gerechtelijk Wetboek, meent de regering dat de arbeidsauditeur geschrapt kan worden uit dit artikel.

wifi, etc.), par exemple en activant le mode avion ou en exploitant l’appareil dans un “environnement Faraday”. De cette manière, on est certain que seules les données sauvegardées dans l’appareil même seront exploitées.

Au point 10 de son avis, le Conseil d’État demande si le fait que chaque liaison externe doive être désactivée par les services de police ne devrait pas être inséré dans le texte même du projet. Le gouvernement estime utile d’accéder à cette demande et a donc ajouté un troisième alinéa au § 2, selon lequel les recherches visées dans ce paragraphe ne peuvent s’étendre qu’aux données sauvegardées dans le système informatique saisi ou non.

Partant de ce raisonnement, s’ils ont désactivé toutes les liaisons externes du système informatique, les services de police peuvent, sans l’autorisation d’un magistrat, également *ouvrir des apps* installées sur ce système. Ils peuvent, par exemple, ouvrir l’application Facebook, les applications de courrier électronique (comme Hotmail, Gmail...) et les applications de messagerie (comme Whatsapp, Viber...) et lire les données, dont les e-mails et les messages textuels. En effet, ces données se trouvent principalement sur l’appareil même. Elles peuvent de ce fait être exploitées.

Au point 6 de son avis, le Conseil d’État n’aperçoit pas la raison pour laquelle l’article 39*bis* mentionne tant le procureur du Roi que l’auditeur du travail alors que tel n’est plus le cas dans le reste du projet. Le terme “auditeur du travail” a été inséré dans les articles 39*bis* et 88*quater* par la loi du 6 juin 2010 introduisant le Code pénal social. L’exposé des motifs de cette loi précise qu’ainsi, “l’auditeur du travail a les mêmes pouvoirs que le procureur du Roi. Les inspecteurs sociaux revêtus de la qualité d’officier de police judiciaire pourront assister le ministère public au cours d’une enquête pénale visant plus particulièrement à lutter contre la criminalité informatique” (*Doc. parl.*, Chambre, 2008-2009, n° 52-1666/001, 324).

Le gouvernement est d’accord avec le Conseil d’État pour dire que cela suscite de la confusion. On pourrait en effet tenir un raisonnement *a contrario*, à savoir que l’auditeur du travail n’a aucune autre compétence ou que l’article 39*bis* pourrait être appliqué en excluant le procureur fédéral ou le procureur général. Vu l’article 22 du Code d’instruction criminelle et les articles 152 et 155 du Code judiciaire, le gouvernement est d’avis que l’auditeur du travail peut être supprimé dans cet article.

De forensische analyse van een informaticasysteem wordt bij voorkeur gedaan op een gemaakte forensische back-up van het in beslag genomen informaticasysteem. Er bestaan evenwel omstandigheden – bijvoorbeeld de hoogdringendheid, het gevaar van verlies van data of sporen, doch ook de laagdrempeligheid van een korte verificatie – waarin het verantwoord kan zijn om zgn. *live forensics* toe te passen, zijnde het uitvoeren van een analyse of exploitatie op het in beslag genomen informaticasysteem zelf. In zulk geval is het van belang dat de op te stellen processen-verbaal zeer duidelijk aangeven welke handelingen werden gesteld en welke eventuele manipulaties of alteraties werden aangebracht op het informaticasysteem.

De huidige § 2 van artikel 88*ter* wordt aangepast en geïntegreerd in een nieuwe § 3 van artikel 39*bis* van het Wetboek van strafvordering. Deze paragraaf vormt het derde niveau van de niet-heimelijke zoeking in informaticasystemen en bepaalt de grenzen van de uitbreiding van de zoeking naar informaticasystemen die zich op een andere plaats bevinden.

De Raad van State stelt de vraag of het niet-heimelijke karakter van de zoeking niet beter in de tekst van het ontworpen artikel 39*bis*, § 3 tot uiting zou moeten komen. De regering meent echter dat de niet-heimelijkheid van alle zoekingen die in artikel 39*bis* zijn opgenomen, evenals de uitbreiding ervan, voortvloeit uit artikel 39*bis*, § 7. Deze paragraaf voorziet in de principiële verplichting om de verantwoordelijke van het informaticasysteem op de hoogte te brengen van de zoeking of de uitbreiding ervan, tenzij diens identiteit of woonplaats niet redelijkerwijze achterhaald kan worden. Ook moet deze verantwoordelijke in voorkomend geval een samenvatting meegedeeld worden van de gegevens die zijn gekopieerd, ontoegankelijk gemaakt of verwijderd. Bovendien blijkt het niet-heimelijke karakter *a contrario* uit de samenlezing met het nieuwe artikel 90*ter*, dat voor de zoeking vervat in dat artikel wél expliciet een heimelijk oogmerk vermeldt (§ 1).

De uitbreiding van de zoeking in een informaticasysteem kan voortaan worden bevolen door de procureur des Konings of de arbeidsauditeur.

Deze uitbreiding beoogt bijvoorbeeld de situaties waarin een smartphone in beslag genomen werd en waarin het noodzakelijk blijkt om toegang te krijgen tot de Hotmail-, Facebook- of Dropbox-account waarmee deze smartphone is verbonden. Zoals eerder aangehaald, staat het huidige recht slechts toe aan de instantie die de inbeslagneming van het toestel bevolen heeft om een zoeking uit te voeren in het toestel zelf, dus niet ten aanzien van de gegevens waarmee het apparaat is verbonden in – bijvoorbeeld – de cloud.

L'analyse judiciaire d'un système informatique s'effectue de préférence sur une duplication du système informatique saisi. Toutefois, dans certaines circonstances – par exemple l'extrême urgence, le risque de perte de données ou de traces, mais également la facilité d'accès d'une brève vérification – il peut être justifié d'appliquer des *live forensics*, c'est-à-dire de procéder à une analyse ou à une exploitation sur le système informatique saisi même. En pareil cas, il importe d'indiquer très clairement dans le procès-verbal à rédiger les opérations effectuées et les manipulations et altérations éventuelles auxquelles il a été procédé dans le système informatique.

L'actuel § 2 de l'article 88*ter* est adapté et intégré dans un nouveau § 3 de l'article 39*bis* du Code d'instruction criminelle. Ce paragraphe forme le troisième niveau de la recherche non secrète dans des systèmes informatiques et fixe les limites de l'extension de la recherche non secrète dans des systèmes informatiques qui se trouvent à un autre endroit.

Le Conseil d'État se pose la question de savoir s'il ne vaudrait pas mieux que le caractère non secret de la recherche apparaisse dans le texte de l'article 39*bis*, § 3, en projet. Le gouvernement est toutefois d'avis que le caractère non secret de toutes les recherches figurant dans l'article 39*bis*, ainsi que de l'extension de celles-ci, découle de l'article 39*bis*, § 7. Ce paragraphe prévoit l'obligation de principe d'informer le responsable du système informatique de la recherche ou de l'extension de la recherche, sauf si son identité ou son adresse ne peuvent être raisonnablement retrouvées. Ce responsable doit également recevoir, le cas échéant, un résumé des données qui ont été copiées, rendues inaccessibles ou retirées. En outre, le caractère non secret ressort *a contrario* de la lecture conjointe avec le nouvel article 90*ter*, lequel mentionne bel et bien explicitement (§ 1er) un but secret pour la recherche visée à cet article.

L'extension de la recherche dans un système informatique peut désormais être ordonnée par le procureur du roi ou l'auditeur du travail.

Cette extension vise par exemple les situations où un smartphone a été saisi et où il apparaît nécessaire d'avoir accès au compte Hotmail, Facebook ou Dropbox auquel ce smartphone est connecté. Comme indiqué précédemment, le droit actuel permet seulement à l'autorité qui a décidé la saisie de l'appareil de faire une recherche dans l'appareil lui-même, pas dans les données auxquelles cet appareil est connecté dans le cloud par exemple.

Ofschoon de tussenkomst van de onderzoeksrechter een essentiële waarborg inhoudt bij het inbreken op de privacy, is de wetwijziging verantwoord omdat artikel 39*bis* zich beperkt tot de niet-heimelijke zoekingen. Artikel 39*bis* wordt zoals gezegd reactief gebruikt naar aanleiding van het feit dat op een wettige wijze de hand kon worden gelegd op een informaticasysteem. De privacy van personen wordt op geen enkele wijze heimelijk benaderd of geëxploiteerd. In die omstandigheden is de controle van de parketmagistraat een voldoende waarborg.

Het heimelijk inbreken op een informaticasysteem en het onder bewaking stellen ervan blijft daarentegen onderworpen aan de tussenkomst van de onderzoeksrechter, thans overeenkomstig artikel 90*ter* e.v. of artikel 89*ter* van het Wetboek van Strafvordering.

Daarnaast is de overdracht van deze maatregel (namelijk de uitbreiding van de zoeking) van artikel 88*ter* naar artikel 39*bis*, en dus van de onderzoeksrechter naar de procureur des Konings, gerechtvaardigd door het feit dat, wegens de ontwikkeling van nieuwe technologieën, het onderscheid tussen hetgeen zich op het toestel bevindt en hetgeen zich in de cloud bevindt voor een deel artificieel wordt.

Evenwel moet deze wijziging samengelezen worden met de nieuwe paragraaf 5 die het gebruik betreft van "valse sleutels" en dergelijke om toegang te krijgen tot de gegevens. De laatste alinea van paragraaf 5 voorziet dat enkel de onderzoeksrechter het gebruik van "valse sleutels" kan bevelen, in het kader van de specifieke toepassing van § 3.

Voorbeeld: de procureur des Konings heeft het gebruik van "valse sleutels" bevolen om de inhoud van een inbeslaggenomen smartphone te doorzoeken. Na zich op deze manier toegang te hebben verschaft tot de smartphone, en op basis van een beslissing van de procureur des Konings met toepassing van paragraaf 3, mogen de speurders het deel van de Gmail- of Dropbox-account van de gebruiker raadplegen dat zich in de cloud bevindt, indien deze accounts rechtstreeks toegankelijk zijn, dus bijvoorbeeld indien deze accounts niet bij elke nieuwe verbinding het ingeven van een wachtwoord vereisen. Daarentegen volstaat de beslissing van de procureur des Konings niet, indien men nieuwe "valse sleutels" moet gebruiken om de maatregel van paragraaf 3 toe te passen, bijvoorbeeld indien men een nieuw paswoord nodig heeft om verbinding te maken met een VPN-netwerk van het bedrijf waarvoor de gebruiker van de smartphone werkt. In een dergelijke situatie is een beslissing van de onderzoeksrechter noodzakelijk.

Même si l'intervention du juge d'instruction inclut une garantie essentielle en matière d'intrusion dans la vie privée, la modification de loi est justifiée parce que l'article 39*bis* se limite aux recherches non secrètes. Comme il a été dit, l'article 39*bis* est utilisé de manière réactive à la suite du fait que l'on a pu s'emparer légalement d'un système informatique. Il n'y a en aucun cas d'approche ou d'exploitation secrète d'éléments de la vie privée des personnes. Dans ces circonstances, le contrôle du magistrat de parquet offre une garantie suffisante.

En revanche, la pénétration en secret dans un système informatique et sa mise sous surveillance restent soumises à l'intervention du juge d'instruction, conformément aux articles 90*ter* et suivants ou à l'article 89*ter* du Code d'instruction criminelle.

Par ailleurs, le transfert de cette mesure (c'est-à-dire l'extension de la recherche) de l'article 88*ter* vers l'article 39*bis* et donc du juge d'instruction vers le procureur du Roi se justifie par le fait que, avec le développement des nouvelles technologies, la distinction entre ce qui se trouve sur l'appareil et ce qui se trouve dans le cloud devient en partie artificielle.

Toutefois, cette modification doit être lue en combinaison avec le nouveau paragraphe 5 qui concerne l'utilisation de "fausses clés" etc. pour accéder aux données. Le dernier alinéa du paragraphe 5 prévoit que seul le juge d'instruction peut ordonner l'usage de "fausses clés" dans le cadre de l'application spécifique du § 3.

Exemple: le procureur du Roi a ordonné l'usage de "fausses clés" pour explorer le contenu d'un smartphone qui a été saisi. Etant ainsi "entrés" dans le smartphone, et sur base d'une décision du procureur du Roi en application du paragraphe 3, les enquêteurs peuvent consulter la partie du compte Gmail ou Dropbox de l'utilisateur du smartphone située dans le cloud si ces comptes sont immédiatement accessibles et donc par exemple si ces comptes ne nécessitent pas l'entrée d'un mot de passe à chaque nouvelle connexion. Par contre, la décision du procureur du Roi ne suffit pas s'il faut utiliser de nouvelles "fausses clés" pour appliquer la mesure du paragraphe 3, par exemple s'il faut un nouveau mot de passe pour se connecter au réseau VPN de l'entreprise pour laquelle l'utilisateur du smartphone travaille. Dans une telle situation, une décision du juge d'instruction est nécessaire.

Na een vraag hieromtrent van de Raad van State, wordt deze situatie uitgebreider toegelicht. Het is belangrijk om het verschil aan te duiden tussen de "nieuwe valse sleutels" en de valse sleutels (bv. een wachtwoord) die vereist waren om toegang te krijgen tot het informaticasysteem zelf, zoals voorzien in § 5 van het ontwerp. Elk additionele gebruik van valse sleutels dat vereist is teneinde de uitbreiding van de zoeking (conform § 3 van artikel 39*bis*) te kunnen uitvoeren, vereist een machtiging van de onderzoeksrechter. Dit is eveneens het geval indien het paswoord, nodig voor de uitbreiding van de zoeking (§ 3), hetzelfde zou blijken te zijn als het paswoord dat nodig was om toegang te krijgen tot het informaticasysteem zelf (§ 2).

Om het met andere woorden te stellen: voor de uitbreiding van een zoeking zal het verplicht zijn zich te wenden tot de onderzoeksrechter wanneer een nieuwe poging tot decodering of "hacking" nodig is bovenop deze die nodig was om binnen te dringen in het informaticasysteem.

Voorbeeld: zo is er geen nieuwe poging tot decryptie of "hacking" vereist om toegang te verkrijgen tot de Facebook-account via de Facebook-app op de smartphone die inbeslaggenomen is en waartoe de speurders toegang hebben kunnen verkrijgen (hetzij omdat deze smartphone niet beveiligd was, hetzij omdat ze erin geslaagd zijn, met machtiging van de procureur des Konings, het toestel te "hacken" en er zo in binnen te dringen). De procureur des Konings kan dus de kennisname bevelen van de Facebookgegevens die zich reeds op de smartphone bevinden op het moment van de inbeslagname, maar hij kan ook het bijwerken (updaten) van de Facebookgegevens bevelen en dus de kennisname van de gegevens die misschien nog niet fysiek op de smartphone staan op het moment van de inbeslagneming ervan. Het feit dat het wachtwoord hetzelfde of verschillend is, is niet van belang. Het doorslaggevend criterium is de (al dan niet) noodzaak om een wachtwoord in te geven op het moment dat de speurders toegang willen verkrijgen tot de gegevens van de "cloud". Indien het wachtwoord door het informaticasysteem "onthouden" werd, en dus niet meer moet ingegeven worden, moet er geen nieuwe stap genomen worden en kan de procureur de uitbreiding van de zoeking machtigen. Indien men daarentegen opnieuw een wachtwoord moet ingeven (zelfs indien het in werkelijkheid om hetzelfde wachtwoord gaat dat gebruikt werd om de toegang tot het besturingssysteem van de smartphone te beveiligen), is voor de uitbreiding naar de gegevens in de "cloud" een machtiging van de onderzoeksrechter vereist.

Dit is enkel het geval voor de gegevens die zich niet bevinden op het informaticasysteem dat

À la suite d'une question posée par le Conseil d'État à ce propos, cette situation est commentée plus en détail. Il importe d'établir la distinction entre les "nouvelles fausses clés" et les fausses clés (p. ex., un mot de passe) qui étaient requises pour obtenir l'accès au système informatique même, comme le prévoit le § 5 du projet. Toute utilisation supplémentaire de fausses clés requise afin de pouvoir étendre la recherche (conformément au § 3 de l'article 39*bis*) nécessite une autorisation du juge d'instruction. Tel est également le cas lorsque le mot de passe nécessaire pour l'extension de la recherche (§ 3) s'avère identique au mot de passe qui était nécessaire pour accéder au système informatique même (§ 2).

En d'autres termes, pour l'extension d'une recherche, il sera obligatoire de s'adresser au juge d'instruction lorsqu'une nouvelle tentative de décodage ou "hacking" est nécessaire en plus de celle qui était nécessaire pour pénétrer dans le système informatique.

Exemple: aucune nouvelle tentative de décryptage ou de "hacking" n'est ainsi requise pour obtenir l'accès au compte Facebook via l'application Facebook sur le smartphone saisi et auquel les enquêteurs ont pu avoir accès (soit parce que le smartphone n'était pas sécurisé, soit parce qu'ils sont parvenus, avec l'autorisation du procureur du Roi, à "hacker" l'appareil pour y accéder). Le procureur du Roi peut donc ordonner la prise de connaissance de données Facebook qui se trouvent déjà dans le smartphone au moment de la saisie, mais il peut également ordonner la mise à jour des données Facebook et donc la prise de connaissance des données qui ne se trouvent peut-être pas encore physiquement dans le smartphone au moment de sa saisie. Le fait que le mot de passe soit identique ou différent importe peu. Le critère déterminant est la nécessité (ou non) d'introduire un mot de passe au moment où les enquêteurs veulent avoir accès aux données du "cloud". Si le mot de passe a été "retenu" par le système informatique et ne doit donc plus être introduit, aucune nouvelle démarche ne doit être entreprise et le procureur peut autoriser l'extension de la recherche. Si, au contraire, un mot de passe doit à nouveau être introduit (même s'il s'agit en réalité du même mot de passe qui a été utilisé pour sécuriser l'accès au système d'exploitation du smartphone), une autorisation du juge d'instruction est requise pour l'extension aux données qui se trouvent sur le "cloud".

Cela ne vaut que pour les données qui ne sont pas situées dans le système informatique qui a été saisi

inbeslaggenomen werd of dat inbeslaggenomen zou kunnen worden. Indien, naast de valse sleutels die nodig waren om toegang te krijgen tot de algemene inhoud van het informaticasysteem, het gebruik van bijkomende "valse sleutels" nodig is om toegang te krijgen tot welbepaalde specifieke delen van het *intern geheugen* van het informaticasysteem, blijft de procureur des Konings bevoegd om het dergelijk gebruik van valse sleutels te bevelen.

Op basis van de artikelen 56, § 2 en 89*bis* van het Wetboek van strafvordering, kan de onderzoeksrechter de opdracht tot uitbreiding van de netwerkzoeking geven aan een officier van gerechtelijke politie van zijn eigen arrondissement of van een ander arrondissement.

In een nieuw laatste lid bij § 3 wordt gesteld dat de procureur des Konings in geval van uiterst dringende noodzakelijkheid of in geval van heterdaad de uitbreidingen van de zoeking mondeling kan bevelen. Dit bevel wordt zo snel mogelijk schriftelijk bevestigd met bevestiging van de heterdaadsituatie of van de redenen van de uiterst dringende noodzakelijkheid.

Paragraaf 4: het vierde niveau betreft een restcategorie, namelijk de informaticasystemen die niet bedoeld zijn in de § § 2 en 3. In dat geval is voor de zoeking de machtiging van een onderzoeksrechter nodig, in voorkomend geval in het kader van de mini-instructie, en moet aan twee voorwaarden voldaan zijn: enerzijds moet de zoeking noodzakelijk zijn voor de waarheidsvinding en anderzijds moet er sprake zijn van proportionaliteit of een risico op het verloren gaan van bewijselementen. Laatstgenoemde voorwaarden zijn *mutatis mutandis* overgenomen uit § 3, eerste lid.

Wanneer de onderzoeksrechter op basis van § 4 een uitbreiding van zijn zoeking beveelt, zijn uiteraard de voorwaarden van § 3 van toepassing. Zo mag de uitbreiding van deze zoeking zich niet verder uitstrekken dan tot de informaticasystemen of de delen ervan waartoe de personen die gerechtigd zijn het informaticasysteem te gebruiken, in het bijzonder toegang hebben.

De maatregel kan bij uiterst dringende noodzakelijkheid mondeling worden bevolen.

Voorbeeld: de onderzoekers weten, bijvoorbeeld via bijzondere opsporingsmethoden, dat de verdachte een Gmail-account heeft, maar hebben geen enkel toestel in beslag genomen dat verbonden is aan die Gmail-account, waardoor de uitbreiding van de zoeking bedoeld in paragraaf 3 niet toepasselijk is.

Door de invoeging van een nieuwe paragraaf 5 wordt verduidelijkt dat de procureur des Konings of

ou qui pourrait être saisi. Si l'usage de "fausses clés" additionnelles à celles pour accéder au contenu général du système informatique est nécessaire pour accéder à certaines parties spécifiques du *stockage interne* du système informatique, le procureur du Roi reste compétent ordonner l'usage de ces "fausses clés".

Sur la base des articles 56, § 2, et 89*bis* du Code d'instruction criminelle, le juge d'instruction peut charger un officier de police judiciaire de son propre arrondissement ou d'un autre arrondissement de procéder à l'extension de la recherche en réseau.

Le dernier alinéa, nouveau, du § 3 prévoit qu'en cas d'extrême urgence ou de flagrant délit, le procureur du Roi peut ordonner oralement les extensions de la recherche. Cet ordre est confirmé par écrit dans les meilleurs délais, avec confirmation du flagrant délit ou des motifs de l'extrême urgence.

Paragraphe 4: le quatrième niveau concerne une catégorie résiduelle, à savoir les systèmes informatiques non visés aux paragraphes 2 et 3. Dans ce cas, la recherche nécessitera l'autorisation d'un juge d'instruction, le cas échéant dans le cadre de la mini-instruction, et deux conditions doivent être remplies: la recherche doit être nécessaire pour la manifestation de la vérité et il doit être question de proportionnalité ou d'un risque de perte d'éléments de preuve. Les conditions précitées sont reprises *mutatis mutandis* du § 3, alinéa 1er.

Lorsque le juge d'instruction ordonne une extension de sa recherche sur la base du § 4, les conditions d'application sont naturellement celles du § 3. Ainsi, l'extension de cette recherche ne peut excéder les systèmes informatiques ou les parties de tels systèmes auxquels ont spécifiquement accès les personnes autorisées à utiliser le système informatique.

La mesure peut en extrême urgence être ordonnée verbalement.

Exemple: les enquêteurs savent, par exemple via des méthodes particulières de recherche, que le suspect a un compte Gmail mais n'ont saisi aucun appareil connecté à ce compte Gmail de sorte que l'extension de la recherche visée au paragraphe 3 n'est pas applicable.

Par l'ajout d'un nouveau paragraphe 5, il est clarifié que le procureur du Roi ou le juge d'instruction peut

de onderzoeksrechter kan bevelen dat in de systemen die het voorwerp uitmaken van een zoeking wordt ingebroken, desgevallend met behulp van technische hulpmiddelen, valse signalen, valse sleutels of valse hoedanigheden. De begrippen "valse signalen" en "valse sleutels" slaan op elk middel dat gebruikt wordt met als doel het omzeilen of kraken van de beveiliging van een informaticasysteem of een deel ervan, teneinde – in leesbare vorm – toegang te verkrijgen tot de gegevens die het systeem bevat. Zo kan bijvoorbeeld een gekraakt paswoord als een valse sleutel worden beschouwd. Met "het opheffen van elke beveiliging" wordt niet bedoeld het ingeven van een correct paswoord.

Uiteraard is het zo dat de onderzoeksrechter alles kan doen wat de procureur des Konings kan op basis van artikel 56, § 1 van het Wetboek van strafvordering. Niettemin is het noodzakelijk om de onderzoeksrechter hier expliciet te vermelden, omdat anders de indruk zou kunnen ontstaan dat de procureur des Konings de maatregel bedoeld in § 5 kan bevelen, ook wanneer het de onderzoeksrechter is die een zoeking heeft bevolen overeenkomstig § 4. Dit is uiteraard niet het geval.

Inbreken in een informaticasysteem is voornamelijk noodzakelijk indien de verdachte weigert om de toegangscode mee te delen, doch dit kan zich ook opdringen indien men op een regelmatige wijze bijvoorbeeld een smartphone, tablet of laptop in beslag genomen heeft zonder dat de eigenaar gekend is.

Dit maakt het onder meer mogelijk paswoorden of het antwoord op geheime vragen te raden, wachtwoorden te kraken, wachtwoorden te gebruiken die hackers hebben bekomen en nadien hebben verspreid via hackerfora, virussen/malware in te zetten, kwetsbaarheden in een systeem uit te buiten, etc.

Onder het begrip "valse sleutels" worden ook vingerafdrukken of andere biometrische gegevens begrepen. Dit laat opsporingsdiensten toe een vingerafdruk, bijvoorbeeld uit een gegevensbank, aan te wenden om zich toegang te verschaffen tot een informaticasysteem. Men denke in dit verband bijvoorbeeld aan smartphones die uitgerust zijn met vingerafdrukbeveiliging.

Ook kunnen technische middelen in de informaticasystemen aangebracht worden om toegang te verkrijgen, in verstaanbare vorm, tot de gegevens die zich erin bevinden of die erdoor verwerkt of doorgestuurd zijn.

De verdachte moet niet eerst de kans worden geboden om diens toegangscode zelf in te geven. Dit zou immers het risico inhouden dat de verdachte, door een

ordonner de pénétrer, le cas échéant à l'aide de moyens techniques, de faux signaux, de fausses clés ou de fausses qualités, dans les systèmes qui font l'objet d'une recherche. Les notions de "faux signaux" et de "fausses clés" se réfèrent à tout moyen utilisé dans le but de contourner ou de craquer la sécurité d'un système informatique ou d'une partie de celui-ci afin d'obtenir l'accès – sous forme lisible – aux données contenues dans ce système. Ainsi, un mot de passe craqué peut notamment être considéré comme une fausse clé. Par "la suppression de toute protection", il n'est pas entendu l'entrée d'un mot de passe correct.

Naturellement, le juge d'instruction est habilité à poser tous les actes que le procureur du Roi peut poser sur la base de l'article 56, § 1er, du Code d'Instruction criminelle. Il est néanmoins nécessaire de mentionner explicitement ici le juge d'instruction, car, dans le cas contraire, cela pourrait donner l'impression que le procureur du Roi peut ordonner la mesure visée au § 5, également lorsque le juge d'instruction a ordonné une recherche conformément au § 4. Cela n'est naturellement pas le cas.

Pénétrer par effraction dans un système informatique est essentiellement nécessaire si le suspect refuse de communiquer le code d'accès, mais cela peut également s'imposer si par exemple un smartphone, une tablette ou un laptop a été saisi de manière régulière sans que l'identité de son propriétaire soit connue.

Cela permet notamment de deviner des mots de passe ou la réponse à des questions secrètes, de craquer des mots de passe, d'utiliser des mots de passe obtenus par les hackers et diffusés ensuite sur des forums de hackers, d'introduire des virus/logiciels malveillants, d'exploiter des faiblesses dans un système...

La notion de "fausses clés" comprend également les empreintes digitales ou autres données biométriques. Cela permet aux services de recherche d'utiliser une empreinte digitale, provenant par exemple d'une banque de données, pour s'introduire dans un système informatique. Pensons par exemple à cet égard aux smartphones équipés d'une protection par empreinte digitale.

Des moyens techniques peuvent également être appliqués aux systèmes informatiques pour obtenir un accès, sous une forme compréhensible, aux données qui s'y trouvent ou qui sont traitées ou transmises par ces systèmes informatiques.

Le suspect ne doit pas se voir d'abord offrir la possibilité d'introduire lui-même ce code d'accès. En effet, cela impliquerait le risque de voir le suspect effacer les

snelle manipulatie of door het ingeven van een verkeerde code, de gegevens op het informaticasysteem wist.

De inhoud van de vroegere § 2 wordt licht gewijzigd overgenomen in de nieuwe § 6.

In het vierde lid van § 6 wordt de mogelijkheid ingeschreven voor de procureur des Konings of de arbeidsauditeur om bepaalde aan een misdrijf gelinkte gegevens te verwijderen, na hiervan kopie te hebben genomen. Dit vormt een extra middel om op te treden tegen bijvoorbeeld kinderpornografie. Een dergelijke mogelijkheid om gegevens te verwijderen is expliciet voorzien in de Richtlijn 2011/93/EU van 13 december 2011 ter bestrijding van seksueel misbruik en de seksuele uitbuiting van kinderen.

In uitvoering van deze Richtlijn, die de lidstaten tevens de verplichting oplegt om websites met kinderpornografisch materiaal "onverwijld" te kunnen laten verwijderen, wordt een zesde lid aan § 6 van artikel 39*bis* Sv. toegevoegd. Deze bepaling laat toe dat de procureur des Konings in geval van uiterst dringende noodzakelijkheid en wanneer het kennelijk gaat om kinderpornografie, de politiediensten *mondeling* machtigt om alle passende technische middelen aan te wenden om deze gegevens ontoegankelijk te maken. Deze machtiging moet nadien zo spoedig mogelijk schriftelijk worden bevestigd.

Dezelfde mogelijkheid wordt voorzien wanneer het gaat om de misdrijven voorzien in de artikelen 137, § 3, 6° of 140*bis* van het Strafwetboek, met name de bedreiging om een terroristische daad te plegen of het aanzetten om één van deze midrijven te plegen.

Deze nieuwe bepaling maakt het mogelijk om kort op de bal te spelen, zonder dat het blokkeren van websites een autonome bevoegdheid wordt voor de politiediensten zelf.

In het tweede lid van deze paragraaf 6 wordt gewag gemaakt van de term "passende technische middelen". De Raad van State verwijst naar zijn advies nr. 28 029/2 van 31 mei 1999 over het voorontwerp dat geleid heeft tot de wet inzake informaticacriminaliteit, en meent dat deze woorden duidelijker gedefineerd moeten worden. Er kan opnieuw worden verwezen naar de memorie van toelichting bij deze wet (*Parl. St.*, Kamer, DOC 0213/001, p.22). Het advies gaat voorbij aan de specificiteit van de evolutie van de informatietechnologie:

— het gaat om technische middelen, en derhalve is de aard daarvan afhankelijk van de stand van de technologie, evenals van de specifieke vereisten van de data;

données dans le système informatique par une manipulation rapide ou l'introduction d'un code erroné.

Le contenu de l'ancien § 2 est repris sous une forme légèrement modifiée dans le nouveau § 6.

L'alinéa 4 du § 6 prévoit la possibilité pour le procureur du roi ou l'auditeur du travail de retirer certaines données liées à une infraction, après en avoir pris copie. Il s'agit d'un moyen d'action supplémentaire contre, par exemple, la pornographie enfantine. Une telle possibilité de retirer les données est explicitement prévue dans la Directive 2011/93/UE du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants.

En exécution de cette directive, qui impose également aux États membres l'obligation de pouvoir faire supprimer "rapidement" les sites internet contenant du matériel pédopornographique, un sixième alinéa est ajouté au § 6 de l'article 39*bis* du Code d'instruction criminelle. Cette disposition prévoit qu'en cas d'extrême urgence et s'il s'agit manifestement de pornographie enfantine, le procureur du Roi peut autoriser *oralement* l'officier de police judiciaire à utiliser tous les moyens techniques appropriés pour rendre ces données inaccessibles. Cette autorisation doit ensuite être confirmée par écrit dans les meilleurs délais.

Cette même possibilité est prévue lorsqu'il s'agit d'infractions prévues à l'article 137, § 3, 6°, ou 140*bis* du Code pénal, à savoir la menace de commettre un attentat terroriste ou l'incitation à commettre l'une de ces infractions.

Cette nouvelle disposition permet de réagir rapidement, sans que le blocage de sites internet devienne une compétence autonome des services de police mêmes.

L'alinéa 2 de ce paragraphe 6 mentionne le terme "moyens techniques appropriés". Le Conseil d'État renvoie à son avis n° 28 029/2 du 31 mai 1999 sur l'avant-projet qui a abouti à la loi relative à la criminalité informatique et est d'avis que ces mots doivent être définis plus clairement. Il peut être renvoyé une nouvelle fois à l'exposé des motifs de cette loi (*Doc. parl.*, Chambre, n° 0213/001, p. 22). L'avis ne prend pas en considération la spécificité de l'évolution de la technologie de l'information:

— il s'agit de moyens techniques et, par conséquent, leur nature dépend de l'état de la technologie ainsi que des exigences spécifiques des données;

— deze middelen hebben als zodanig geen effect op de bewijswaarde van de data, maar betreffen de modaliteiten van de onttrekking of bewaring van de data, waardoor nodeloze bewijsbetwistingen voor de rechter kunnen worden voorkomen;

— bovendien gaat het hier om een wettelijke vereiste met het oog op het beschermen van het bewijsmateriaal; deze bestaat zelfs niet in het gemeen recht, en werd ingevoegd omwille van de eigenheid van de geïnformatiseerde omgeving.

De paragrafen 7 en 8 zijn overgenomen uit het huidige artikel 39*bis* en werden slechts punctueel aangepast. Aan § 7 wordt toegevoegd dat de mededeling aan de verantwoordelijke van het informaticasysteem niet dient te gebeuren indien zijn identiteit of woonplaats redelijkerwijze niet achterhaald kan worden, zoals nu ook voorzien is in het huidige artikel 88*ter*. Op vraag van de Raad van State (punt 16 *in fine* van het advies) wordt ook de onderzoeksrechter hier ingevoegd.

Op suggestie van de Raad van State wordt nu in § 7 verduidelijkt dat de verantwoordelijke van het informaticasysteem zo spoedig mogelijk op de hoogte moet worden gebracht van de zoeking.

De Raad van State meent eveneens (en verwijst in dat opzicht naar advies nr. 28 029/2 van 31 mei 1999) dat deze "verantwoordelijke van het informaticasysteem" in de tekst van het voorontwerp zelf moet worden omschreven. De bedoeling van het op de hoogte brengen van de maatregel is evenwel duidelijk te stellen dat het niet gaat om een geheime maatregel (vergelijk met de huiszoekingsbevoegdheid). De terminologie in het voorontwerp behoudt in dat opzicht enige flexibiliteit aangaande de te contacteren persoon: het kan inderdaad niet in alle gevallen *a priori* eenduidig vastgesteld worden wie de reële of juridische controle heeft over het systeem (*Parl.St.* Kamer 1999-2000, nr. 0213/001, 21).

In voorkomend geval zal ook een samenvatting van de gekopieerde, ontoegankelijk gemaakte of verwijderde gegevens meegedeeld moeten worden. De woorden "in voorkomend geval" betekenen niet dat dit aan het oordeel van de magistraat in kwestie wordt overgelaten. Ze wijzen er alleen op dat de mededeling enkel dient te gebeuren indien effectief gegevens gekopieerd werden. Uiteraard zal er ook geen mededeling zijn als de verantwoordelijke van het informaticasysteem niet gekend is.

Artikel 3

Het nieuwe artikel 39*ter* belichaamt de omzetting van de artikelen 16 en 17 van de Cybercrimeconventie

— ces moyens n'ont en tant que tels aucun effet sur la valeur probante des données, mais concernent les modalités d'extraction ou de conservation des données qui permettent de prévenir des contestations de preuve inutiles devant le juge;

— en outre, il s'agit en l'occurrence d'une exigence légale en vue de la protection des preuves; elle n'existe même pas dans le droit commun et a été insérée en raison de la particularité de l'environnement informatisé.

Les paragraphes 7 et 8 proviennent du présent article 39*bis* et ont uniquement fait l'objet d'adaptations ponctuelles. Dans le § 7, il est ajouté que le responsable du système informatique ne doit pas être informé si son identité ou son adresse ne peuvent être raisonnablement retrouvées, comme le prévoit également désormais le présent article 88*ter*. À la demande du Conseil d'État (point 16 *in fine* de l'avis), le juge d'instruction est également inséré ici.

À la suggestion du Conseil d'État, il est à présent précisé au § 7 que le responsable du système informatique doit être informé de la recherche dans les plus brefs délais.

Le Conseil d'État estime également (et renvoie à cet égard à l'avis n° 28 029/2 du 31 mai 1999) que le texte de l'avant-projet de loi doit lui-même contenir une définition du "responsable du système informatique". Le but de la communication de la mesure est toutefois d'établir clairement qu'il ne s'agit pas d'une mesure secrète (cf. la compétence de perquisitionner). La terminologie de l'avant-projet comporte dans cette optique une certaine souplesse pour ce qui est de la personne à contacter: en effet, il n'est pas possible de déterminer *a priori* pour tous les cas et de manière univoque qui exerce le contrôle réel ou juridique sur le système (*Doc. parl.*, Chambre, 1999-2000, n° 0213/001, 21).

Le cas échéant, un résumé des données qui ont été copiées, rendues inaccessibles ou retirées devra également être communiqué. Les mots "le cas échéant" ne signifient pas que cela est laissé à l'appréciation du magistrat en question. Ils signifient uniquement que la communication devra être faite uniquement lorsque des données ont effectivement été copiées. Bien entendu, il n'y aura pas non plus de communication lorsque le responsable du système informatique n'est pas connu.

Article 3

Le nouvel article 39*ter* matérialise la transposition des articles 16 et 17 de la Convention sur la cybercriminalité

van 23/11/2001 (hierna ook "CC") met betrekking tot de snelle bewaring en onthulling van gegevens (nationaal).

De draagwijdte van de artikelen 16 en 17 CC:

Aan de hand van een paar uittreksel uit het Toelichtend Verslag bij de Cybercrimeconventie kan de draagwijdte van de artikelen juist geïnterpreteerd worden. Het Toelichtend Verslag begint met een algemene uitleg over de twee artikelen, met daarin oa de volgende passages:

"Les articles 16 et 17 prévoient donc uniquement le pouvoir de requérir la conservation de données stockées existantes, en attendant la divulgation des données en application d'autres pouvoirs juridiques, à l'occasion d'enquêtes ou de procédures pénales spécifiques.

(…)

L'un des moyens de préserver l'intégrité des données consiste pour les autorités compétentes à opérer des perquisitions ou à accéder d'une autre manière aux données et à saisir les données ou à se les procurer d'une autre manière. Toutefois, lorsque le gardien des données est digne de confiance, comme dans le cas d'une entreprise ayant une bonne réputation, l'intégrité des données peut être garantie plus rapidement au moyen d'une injonction de conserver les données. Une injonction d'avoir à conserver les données peut être moins perturbatrice pour les activités et moins préjudiciable à la réputation d'une entreprise honnête qu'une opération de perquisition de ses locaux aux fins de saisie.

(…)

Le pouvoir de conservation rapide des données informatiques doit permettre de faire face à ces problèmes. Les Parties sont donc invitées à instaurer le pouvoir d'ordonner la conservation de données informatiques spécifiées, en tant que mesure provisoire; les données seront conservées durant une période aussi longue que nécessaire, qui pourra aller jusqu'à 90 jours. Les Parties pourront prévoir le renouvellement de cette mesure. Durant la période de conservation, les données ne sont pas automatiquement portées à la connaissance des services répressifs. En effet, pour que les données puissent être divulguées, il faut prendre une mesure supplémentaire de divulgation ou ordonner une perquisition.

(…)

On peut ainsi s'assurer que des données essentielles ne disparaissent pas pendant la longue procédure

concernant la conservation et la divulgation rapides de données informatiques (nationales).

Portée des articles 16 et 17 de la Convention:

Quelques extraits du Rapport explicatif à la Convention sur la cybercriminalité permettent de donner une interprétation correcte à la portée de ces articles. Le Rapport explicatif commence par une explication d'ordre général sur les deux articles contenant notamment les passages suivants:

"Les articles 16 et 17 prévoient donc uniquement le pouvoir de requérir la conservation de données stockées existantes, en attendant la divulgation des données en application d'autres pouvoirs juridiques, à l'occasion d'enquêtes ou de procédures pénales spécifiques.

(…)

L'un des moyens de préserver l'intégrité des données consiste pour les autorités compétentes à opérer des perquisitions ou à accéder d'une autre manière aux données et à saisir les données ou à se les procurer d'une autre manière. Toutefois, lorsque le gardien des données est digne de confiance, comme dans le cas d'une entreprise ayant une bonne réputation, l'intégrité des données peut être garantie plus rapidement au moyen d'une injonction de conserver les données. Une injonction d'avoir à conserver les données peut être moins perturbatrice pour les activités et moins préjudiciable à la réputation d'une entreprise honnête qu'une opération de perquisition de ses locaux aux fins de saisie.

(…)

Le pouvoir de conservation rapide des données informatiques doit permettre de faire face à ces problèmes. Les Parties sont donc invitées à instaurer le pouvoir d'ordonner la conservation de données informatiques spécifiées, en tant que mesure provisoire; les données seront conservées durant une période aussi longue que nécessaire, qui pourra aller jusqu'à 90 jours. Les Parties pourront prévoir le renouvellement de cette mesure. Durant la période de conservation, les données ne sont pas automatiquement portées à la connaissance des services répressifs. En effet, pour que les données puissent être divulguées, il faut prendre une mesure supplémentaire de divulgation ou ordonner une perquisition.

(…)

On peut ainsi s'assurer que des données essentielles ne disparaissent pas pendant la longue procédure

d'entraide judiciaire classique pendant laquelle la Partie requise se procure les données et les remet à la Partie requérante.

(…)".

Uit deze algemene commentaar blijkt dat de snelle bewaring van gegevens niet gelijkgesteld kan worden met een inbeslagneming. Het gaat eerder om een maatregel die snel genomen moet worden om de gegevens in de schoot zelf van de persoon die ze onder zich houdt, te bewaren om te voorkomen dat ze beschadigd geraken of verloren gaan. Op dat moment hebben de gerechtelijke autoriteiten nog geen toegang tot die gegevens. Er wordt enkel gevraagd aan een persoon (of rechtspersoon) om de gegevens gedurende een bepaalde termijn op een veilige manier te bewaren. Het overmaken van de bewaarde gegevens aan de bevoegde gerechtelijke autoriteit verloopt conform de nationale regelgeving ter zake (bv. op grond van artikel 46*bis* of 88*bis* Sv. In het voorontwerp van wet was dit principe ingeschreven in een paragraaf 4 van artikel 39*ter*. Ingevolge een opmerking van de Raad van State werd deze overbodige paragraaf geschrapt.

Er wordt in artikel 39*ter* expliciet gezegd dat het gaat om personen te goeder trouw, en dat een dergelijke maatregel minder vergaand is en dus geen gevolgen zal hebben op de goede reputatie van bedrijven. Zoals verder zal blijken, heeft een maatregel tot snelle bewaring ook weinig zin bij personen te kwader trouw of verdachten.

Uitleg bij artikel 16 CC

Artikel 16 betreft de snelle bewaring van elektronische gegevens in het algemeen, met inbegrip van verkeersgegevens. Enkele passages uit het Toelichtend Verslag:

"La "conservation" exige que les données qui existent déjà et sont stockées soient protégées contre tout ce qui risquerait d'en modifier ou dégrader la qualité ou l'état actuel. Elle exige que les données soient maintenues à l'abri de toute modification, de toute détérioration ou de tout effacement. La conservation n'implique pas nécessairement que les données soient "gelées" (c'est-à-dire rendues inaccessibles) et que ces données ou des copies de ces données ne puissent pas être utilisées par des utilisateurs légitimes. La personne à laquelle est adressée l'injonction peut, en fonction des spécifications exactes de celle-ci, conserver l'accès aux données. L'article ne précise pas la manière dont les données doivent être conservées. Il appartient à chaque Partie d'établir les modalités appropriées de

d'entraide judiciaire classique pendant laquelle la Partie requise se procure les données et les remet à la Partie requérante.

(…)".

Il ressort de ce commentaire général que la conservation rapide des données ne peut être assimilée à une saisie. Il s'agit plutôt d'une mesure qui doit être prise rapidement afin de conserver les données chez la personne même qui les détient pour éviter qu'elles soient endommagées ou perdues. À ce moment, les autorités judiciaires n'ont pas encore accès à ces données. Il est uniquement demandé à une personne (ou une personne morale) de conserver de manière sécurisée les données pendant une période déterminée. La transmission des données conservées à l'autorité judiciaire compétente se déroule conformément à la réglementation nationale en la matière (notamment sur la base de l'article 46*bis* ou 88*bis* du Code d'instruction criminelle. Dans l'avant-projet de loi, ce principe figurait dans un paragraphe 4 de l'article 39*ter*. À la suite d'une remarque du Conseil d'État, ce paragraphe superflu a été supprimé.

À l'article 39*ter*, il est précisé explicitement qu'il s'agit de personnes de bonne foi et qu'une telle mesure a un caractère moins extrême et n'aura donc aucune incidence sur la bonne réputation des entreprises. Comme on le verra plus loin, une mesure de conservation rapide a également peu de sens vis-à-vis de personnes de mauvaise foi ou de suspects.

Explication relative à l'article 16 de la Convention

L'article 16 traite de la conservation rapide de données électroniques en général, y compris les données relatives au trafic. Quelques passages du Rapport explicatif:

"La "conservation" exige que les données qui existent déjà et sont stockées soient protégées contre tout ce qui risquerait d'en modifier ou dégrader la qualité ou l'état actuel. Elle exige que les données soient maintenues à l'abri de toute modification, de toute détérioration ou de tout effacement. La conservation n'implique pas nécessairement que les données soient "gelées" (c'est-à-dire rendues inaccessibles) et que ces données ou des copies de ces données ne puissent pas être utilisées par des utilisateurs légitimes. La personne à laquelle est adressée l'injonction peut, en fonction des spécifications exactes de celle-ci, conserver l'accès aux données. L'article ne précise pas la manière dont les données doivent être conservées. Il appartient à chaque Partie d'établir les modalités appropriées de

conservation et de déterminer si, dans certains cas, la conservation des données devrait également comporter le "gel" de celles-ci.

La mention "ordonner ou ... obtenir par un moyen similaire" vise à autoriser la mise en œuvre d'autres moyens juridiques de conservation que l'injonction judiciaire ou administrative ou une instruction (de la police ou du parquet, par exemple). Dans certains États, le droit de procédure ne prévoit pas d'injonctions de conservation; les données ne peuvent alors être conservées que par la voie d'opérations de perquisition et saisie ou d'une injonction de produire. L'utilisation du membre de phrase "ou ... obtenir par un moyen similaire" introduit la souplesse voulue pour permettre à ces États d'appliquer cet article en mettant en œuvre ces autres moyens. Toutefois, il est recommandé aux États d'envisager d'instaurer des pouvoirs et procédures permettant d'ordonner effectivement au destinataire d'une injonction de conserver les données, car la rapidité de l'intervention de cette personne peut, dans certains cas, permettre d'appliquer plus rapidement les mesures de conservation.(…) La durée, qui ne devrait pas excéder 90 jours, devrait être suffisante pour permettre aux autorités compétentes de prendre d'autres mesures juridiques, telles que la perquisition et la saisie, l'accès aux données ou leur obtention par un moyen similaire, ou l'émission d'une injonction de produire, en vue d'obtenir la divulgation des données.

Pour les services de lutte contre la criminalité, la conservation rapide des données s'inscrit dans le cadre des enquêtes préliminaires, période durant laquelle il peut être important de conserver le secret. La conservation est une mesure préliminaire adoptée en attendant que soient prises d'autres mesures juridiques visant à obtenir les données ou leur divulgation. La confidentialité s'impose pour éviter que d'autres personnes ne tentent de manipuler ou d'effacer les données.".

Uit deze uitleg blijkt dat de snelle bewaring een maatregel is die nog voorafgaat aan verdergaande maatregelen zoals de inbeslagneming of de bevriezing van gegevens.

Ook de volgende passage is van belang:

"Toutefois, si le gardien n'était pas digne de confiance, il serait plus sûr de procéder à la conservation par perquisition et saisie plutôt que par une injonction à laquelle l'intéressé pourrait ne pas obtempérer. Le paragraphe 1 mentionne expressément les "données relatives au trafic" afin d'indiquer l'applicabilité particulière de ces dispositions à ce type de données, lesquelles, lorsqu'elles sont collectées et archivées par un fournisseur de services, ne sont généralement

conservation et de déterminer si, dans certains cas, la conservation des données devrait également comporter le "gel" de celles-ci.

La mention "ordonner ou ... obtenir par un moyen similaire" vise à autoriser la mise en œuvre d'autres moyens juridiques de conservation que l'injonction judiciaire ou administrative ou une instruction (de la police ou du parquet, par exemple). Dans certains États, le droit de procédure ne prévoit pas d'injonctions de conservation; les données ne peuvent alors être conservées que par la voie d'opérations de perquisition et saisie ou d'une injonction de produire. L'utilisation du membre de phrase "ou ... obtenir par un moyen similaire" introduit la souplesse voulue pour permettre à ces États d'appliquer cet article en mettant en œuvre ces autres moyens. Toutefois, il est recommandé aux États d'envisager d'instaurer des pouvoirs et procédures permettant d'ordonner effectivement au destinataire d'une injonction de conserver les données, car la rapidité de l'intervention de cette personne peut, dans certains cas, permettre d'appliquer plus rapidement les mesures de conservation.(…) La durée, qui ne devrait pas excéder 90 jours, devrait être suffisante pour permettre aux autorités compétentes de prendre d'autres mesures juridiques, telles que la perquisition et la saisie, l'accès aux données ou leur obtention par un moyen similaire, ou l'émission d'une injonction de produire, en vue d'obtenir la divulgation des données.

Pour les services de lutte contre la criminalité, la conservation rapide des données s'inscrit dans le cadre des enquêtes préliminaires, période durant laquelle il peut être important de conserver le secret. La conservation est une mesure préliminaire adoptée en attendant que soient prises d'autres mesures juridiques visant à obtenir les données ou leur divulgation. La confidentialité s'impose pour éviter que d'autres personnes ne tentent de manipuler ou d'effacer les données.".

Il ressort de cette explication que la conservation rapide est une mesure qui précède des mesures plus intrusives comme la saisie ou le gel des données.

Le passage suivant est également important:

"Toutefois, si le gardien n'était pas digne de confiance, il serait plus sûr de procéder à la conservation par perquisition et saisie plutôt que par une injonction à laquelle l'intéressé pourrait ne pas obtempérer. Le paragraphe 1 mentionne expressément les "données relatives au trafic" afin d'indiquer l'applicabilité particulière de ces dispositions à ce type de données, lesquelles, lorsqu'elles sont collectées et archivées par un fournisseur de services, ne sont généralement

conservées qu'une brève période. Par ailleurs, la mention des "données relatives au trafic" établit un lien entre les mesures visées aux articles 16 et 17.".

Er wordt dus expliciet gezegd dat het beter is om over te gaan tot een huiszoeking of een inbeslagneming wanneer de houder van de gegevens niet te goeder trouw is en mogelijks niet zou gehoorzamen aan de vraag tot snelle bewaring van de gegevens.

Samengevat: Artikel 16 CC beoogt een snelle bewaring van elektronische gegevens die onder de controle of bewaring zijn van een fysiek of rechtspersoon, door die persoon zelf, en niet door de gerechtelijke autoriteiten. Deze maatregel is dus een bewarende maatregel die zich meestal zal voordoen in het vooronderzoek, en de bedrijven/personen die er het voorwerp van uitmaken zullen meestal ter goeder trouw zijn.

Uitleg bij artikel 17 CC

Artikel 17 is nauw verbonden met artikel 16 en voorziet specifieke verplichtingen voor de snelle bewaring van verkeersgegevens (zoals voorzien in artikel 16) en de overdracht van die gegevens aan de bevoegde autoriteiten. Het doel van dit artikel is de bron of de bestemming van een bepaalde communicatie te kunnen identificeren, wanneer bijvoorbeeld meerde dienstenverstrekkers tussengekomen zijn bij de overdracht van die communicatie.

Het Toelichtend Verslag legt het als volgt uit:

"Il arrive souvent que plusieurs fournisseurs de services participent à la transmission d'une communication. Chaque fournisseur peut posséder certaines données relatives au trafic concernant la transmission de la communication spécifiée, qui ont soit été produites et archivées par ce fournisseur à l'occasion du passage de la communication par son système, soit ont été fournies par d'autres fournisseurs. Il arrive que les données relatives au trafic, ou tout au moins certains types de données relatives au trafic, soient partagées entre les fournisseurs de services ayant participé à la transmission de la communication, à des fins commerciales, sécuritaires ou techniques. En pareil cas, l'un ou l'autre de ces fournisseurs peut posséder les données relatives au trafic essentielles pour déterminer la source ou la destination de la communication. Souvent, toutefois, aucun fournisseur ne possède à lui seul suffisamment de données relatives au trafic pour permettre de déterminer avec exactitude la source ou la destination de la communication. Chacun possède certaines parties du

conservées qu'une brève période. Par ailleurs, la mention des "données relatives au trafic" établit un lien entre les mesures visées aux articles 16 et 17.".

Il est donc précisé explicitement qu'il est préférable de procéder à une perquisition ou à une saisie si le titulaire des données n'est pas de bonne foi et pourrait ne pas donner suite à la demande de conservation rapide des données.

En résumé: L'article 16 de la Convention vise une conservation rapide des données électroniques qui sont sous le contrôle d'une personne physique ou morale, ou conservées par celle-ci, par cette personne même et non par les autorités judiciaires. Il s'agit donc d'une mesure conservatoire qui interviendra généralement au cours de l'enquête préliminaire et les entreprises/personnes qui en font l'objet seront généralement de bonne foi.

Explication relative à l'article 17 de la Convention

L'article 17 est étroitement lié à l'article 16 et prévoit des obligations spécifiques pour la conservation rapide de données relatives au trafic (comme prévu à l'article 16) et le transfert de ces données aux autorités compétentes. Cet article a pour objet de pouvoir identifier la source ou la destination d'une communication spécifiée si, par exemple, plusieurs fournisseurs de services sont intervenus lors de la transmission de cette communication.

Le Rapport explicatif précise ce qui suit:

"Il arrive souvent que plusieurs fournisseurs de services participent à la transmission d'une communication. Chaque fournisseur peut posséder certaines données relatives au trafic concernant la transmission de la communication spécifiée, qui ont soit été produites et archivées par ce fournisseur à l'occasion du passage de la communication par son système, soit ont été fournies par d'autres fournisseurs. Il arrive que les données relatives au trafic, ou tout au moins certains types de données relatives au trafic, soient partagées entre les fournisseurs de services ayant participé à la transmission de la communication, à des fins commerciales, sécuritaires ou techniques. En pareil cas, l'un ou l'autre de ces fournisseurs peut posséder les données relatives au trafic essentielles pour déterminer la source ou la destination de la communication. Souvent, toutefois, aucun fournisseur ne possède à lui seul suffisamment de données relatives au trafic pour permettre de déterminer avec exactitude la source ou la destination de la communication. Chacun possède certaines parties du

puzzle et chacune de ces parties doit être examinée afin d'identifier la source ou la destination.

L'article 17 veille, lorsqu'un seul ou plusieurs fournisseurs de services ont participé à la transmission d'une communication, à ce qu'il soit procédé à la conservation rapide des données relatives au trafic parmi tous les fournisseurs. Il ne précise pas les moyens d'y parvenir, laissant au droit interne le soin de déterminer un moyen compatible avec l'ordre juridique et économique national.".

Samengevat: Artikel 17 CC legt aan de Partijen de verplichting op om de snelle bewaring van verkeersgegevens mogelijk te maken voor een bepaalde communicatie bij verschillende dienstenverstrekkers die deelgenomen hebben aan de transmissie van die communicatie. Het legt ook de verplichting op om een snelle overdracht van die gegevens aan de bevoegde autoriteiten op te leggen, met het oog op de identificatie van de verschillende dienstenverstrekkers die deelgenomen hebben aan de transmissie van de communicatie, van de bron en de bestemming van de communicatie, en van de weg die deze bepaalde communicatie heeft afgelegd.

Verhouding tot artikel 39*bis* van het Wetboek van Strafvordering

Dit artikel vertoont gelijkenissen met de artikelen 16 en 17 CC, maar is toch niet voldoende om deze verplichtingen uit te voeren.

Artikel 39*bis* Sv is een vorm van inbeslagneming van elektronische gegevens opgeslagen in een informaticasysteem waarin de procureur des Konings een zoeking laat uitvoeren, en situeert zich in het opsporingsonderzoek. M.a.w. het is de bevoegde gerechtelijke autoriteit zelf die de gegevens kopieert en eventueel ontoegankelijk maakt. In het geval van artikel 16 CC is het echter de persoon die de gegevens onder zich houdt of controleert, die de gegevens gedurende een bepaalde periode dient te bewaren, met het oog op de latere onthulling ervan aan de bevoegde gerechtelijke autoriteit.

Door het in algemene termen te hebben over "gegevens die opgeslagen, verwerkt of overgedragen worden door middel van een informaticasysteem", zijn ook de verkeersgegevens van artikel 17 CC gedekt.

Artikel 4

Het nieuwe artikel 39*quater* belichaamt de omzetting van de artikelen 29 en 30 van de Cybercrimeconventie

puzzle et chacune de ces parties doit être examinée afin d'identifier la source ou la destination.

L'article 17 veille, lorsqu'un seul ou plusieurs fournisseurs de services ont participé à la transmission d'une communication, à ce qu'il soit procédé à la conservation rapide des données relatives au trafic parmi tous les fournisseurs. Il ne précise pas les moyens d'y parvenir, laissant au droit interne le soin de déterminer un moyen compatible avec l'ordre juridique et économique national.".

En résumé: L'article 17 impose aux parties l'obligation de permettre la conservation rapide des données relatives au trafic pour une communication déterminée chez différents fournisseurs de services qui ont participé à la transmission de cette communication. Il impose également l'obligation de transmettre rapidement ces données aux autorités compétentes, en vue d'identifier les différents fournisseurs de services qui ont participé à la transmission de la communication, la source et la destination de la communication, et le chemin suivi par cette communication.

Relation avec l'article 39*bis* du Code d'instruction criminelle

Cet article présente des similitudes avec les articles 16 et 17 de la Convention mais n'est toutefois pas suffisant pour exécuter ces obligations.

L'article 39*bis* du Code d'instruction criminelle concerne une forme de saisie de données électroniques stockées dans un système informatique dans lequel le procureur du Roi fait procéder à une recherche et s'inscrit dans le cadre de l'information. En d'autres termes, c'est l'autorité judiciaire compétente même qui copie les données et les rend éventuellement inaccessibles. Dans le cas de l'article 16 de la Convention, c'est plutôt la personne qui détient ou qui contrôle les données qui doit les conserver pendant une période déterminée en vue de leur divulgation ultérieure à l'autorité judiciaire compétente.

Les termes généraux "données stockées, traitées ou transmises par le biais d'un système informatique" couvrent également les données relatives au trafic de l'article 17.

Article 4

Le nouvel article 39*quater* matérialise la transposition des articles 29 et 30 de la Convention sur la

met betrekking tot de snelle bewaring en onthulling van gegevens (internationaal).

De Cybercrimeconventie biedt in zijn artikel 29 en 30 een verdragsbasis om een uitzondering te maken op de bestaande rechtshulpverdragen door enerzijds relatief informeel te kunnen verzoeken tot een snelle bewaring van gegevens en anderzijds door zonder rechtshulpverzoek een snelle onthulling van verkeersgegevens te kunnen verkrijgen in de in het verdrag bepaalde gevallen.

De snelle bewaring in het buitenland (artikel 29 CC) is wezenlijk gemaakt om gegevens te bewaren in afwachting van een rechtshulpverzoek. Tal van grote providers werken momenteel zeer goed en efficiënt mee met de FCCU. Er zijn ook andere voorbeelden waarbij de discussie zich afspeelt of de verdragen inzake wederzijdse rechtshulp nu wel gevolgd dienen te worden of niet en of er rechtsgeldig rechtstreeks mag worden meegewerkt.

Om te vermijden dat de nieuwe wet voor gevolg zou hebben dat er discussie ontstaat over het statuut van het verzoek tot "snelle bewaring" dat rechtstreeks ten aanzien van buitenlandse ISP's wordt gestuurd, wordt de eerste paragraaf van artikel 39*quater* als volgt geformuleerd: "Onverminderd de mogelijkheden tot rechtstreekse samenwerking met buitenlandse operatoren van elektronische communicatiediensten en verstrekkers van elektronische communicatiediensten, kan …"

Zo wordt een wettelijk kader gecreëerd voor rechtstreekse samenwerking met buitenlandse ISP's conform de reeds bestaande praktijk.

Artikel 39*quater*, § 1, tweede lid bepaalt de vorm en inhoud van een verzoek om bewaring. Dit is gelijkluidend aan wat er is bepaald in artikel 29.2 van de Conventie.

Artikel 39*quater*, § 2 regelt de procedure als België zelf aangezochte Staat is.

In § 2 is voorzien in een procedure in twee fases: eerst een voorlopige en spoedige bewaring van de gegevens waartoe de politie beslist op grond van het buitenlandse verzoek, vervolgens een beslissing van de gerechtelijke autoriteit inzake het verzoek tot bewaring.

In § 2 is verduidelijkt dat de procedure slechts toepasselijk is als erin is voorzien in een internationaal rechtsinstrument tussen België en de Staat die om bewaring verzoekt. Het begrip "internationaal rechtsinstument" is overgenomen uit de wet van 9 december 2004 betreffende de wederzijdse internationale rechtshulp

cybercriminalité concernant la conservation et la divulgation rapides de données informatiques (internationales).

La Convention sur la cybercriminalité offre en ses articles 29 et 30 une base conventionnelle qui permet de déroger aux conventions d'entraide judiciaire existantes en permettant, d'une part, de demander de manière relativement informelle une conservation rapide des données et, d'autre part, d'obtenir sans demande d'entraide judiciaire la divulgation rapide de données relatives au trafic dans les cas prévus par la Convention.

La conservation rapide à l'étranger (article 29 de la Convention) a essentiellement pour but de conserver des données dans l'attente d'une demande d'entraide judiciaire. De nombreux grands fournisseurs collaborent actuellement de manière très efficace avec la FCCU. Dans d'autres exemples, la discussion porte sur la question de savoir si les conventions d'entraide judiciaire doivent être bien suivies ou non et si une collaboration valable directe est possible.

Pour éviter que la nouvelle loi suscite une discussion sur le statut de la demande de "conservation rapide" envoyée directement aux ISP étrangers, le paragraphe 1er de l'article 39*quater* est formulé comme suit: "Sans préjudice des possibilités de collaboration directe avec des opérateurs de services de communications électroniques et des fournisseurs de services de communications électroniques étrangers, le..."

Un cadre légal est ainsi créé pour une collaboration directe avec des ISP étrangers conformément aux pratiques existantes.

L'article 39*quater*, § 1er, alinéa 2, définit la forme et le contenu d'une demande de conservation. C'est conforme à ce que prévoit l'article 29, 2., de la Convention.

L'article 39*quater*, § 2, règle la procédure si la Belgique est elle-même État requis.

Le § 2 prévoit une procédure en deux temps: d'abord une conservation provisoire et en urgence des données décidée par la police sur base de la demande étrangère, ensuite une décision par l'autorité judiciaire sur la demande de conservation.

Le § 2 précise que la procédure n'est applicable que si elle est prévue dans un instrument de droit international liant la Belgique et l'État qui fait la demande de conservation. La notion d' "instrument de droit international" est reprise de la loi du 9 décembre 2004 sur l'entraide judiciaire pénale et inclut les instruments

in strafzaken en omvat de wetgevende instrumenten van de Europese Unie. Aangezien, in afwachting van de beslissing van de gerechtelijke autoriteit, de procedure waarin is voorzien een heel korte bewaring mogelijk maakt door de politie, is het belangrijk dat zij slechts geldt voor de Staten waarmee België is gebonden. In dat verband moet worden opgemerkt dat de Cybercrimeconventie niet enkel open staat voor de lidstaten van de Raad van Europa. Ook sleutelpartners inzake de bestrijding van cybercriminaliteit, zoals de Verenigde Staten, Canada of Australië zijn er partij bij.

De weigeringsgronden die zijn opgenomen in de artikelen 29.5 en 30.2 van de Conventie staan vermeld in artikel 39*quater*, § 2, vierde lid.

Er is erin voorzien dat de gronden voor het weigeren van samenwerking van toepassing zijn "onverminderd de internationale rechtsinstrumenten met betrekking tot rechtshulp waardoor België gebonden is en die ertoe strekken deze samenwerking te bevorderen". Die formulering is geïnspireerd op artikel 2/3 van de wet van 9 december 2004 betreffende de wederzijdse rechtshulp zoals ingevoegd bij de wet van 15 mei 2014. Het is de bedoeling over een voor verandering vatbaar kader te beschikken en rekening te houden met de meest ambitieuze normen die bijvoorbeeld zouden kunnen worden vastgelegd in het kader van de Europese Unie of op bilateraal vlak en die zouden voorzien in beperktere gronden voor het weigeren van samenwerking. Naar dezelfde wet kan verwezen worden in antwoord op de vraag van de Raad van State naar een nadere omschrijving van het begrip "wezenlijke belangen van België" (punt 21, p. 19 van het advies). Deze woorden worden ook gebruikt in deze wet met betrekking tot de weigeringsgronden voor rechtshulp. De memorie van toelichting bij deze wet stelt hieromtrent: "[H]et gaat om de "clausule van openbare orde" in de ruime zin, zoals verwoord in het Verdrag van 1959 van de Raad van Europa aangaande de wederzijdse rechtshulp in strafzaken. Deze clausule van openbare orde betreft conflicten met de belangen van de Belgische Staat (soevereiniteit, positie op internationaal vlak,...), alsook gevallen waarin, inzonderheid wegens de toestand in de verzoekende Staat, de tenuitvoerlegging in strijd is met de grondbeginselen van de democratie, van de rechtsstaat en van de fundamentele rechten*"* (*Parl.St.* Kamer 2003-04, nr. 1278/001, 9).

Artikel 29.7 van de Cybercrimeconventie voorziet in een minimum bewaringstermijn van 60 dagen. Dit wordt overgenomen in artikel 39*quater*, § 2, 6e lid. Ingeval van een buitenlands verzoek op grond van artikel 29 van de Cybercrimeconventie moeten de gegevens sowieso worden bewaard vanaf dat het (rechtshulp)verzoek

législatifs de l'Union européenne. La procédure prévue permettant une conservation, même très brève, par la police en attendant la décision de l'autorité judiciaire, il est important qu'elle ne soit applicable qu'avec les États auxquels la Belgique est liée. On notera à cet égard que la Convention Cybercrime n'est pas seulement ouverte aux États membres du Conseil de l'Europe. Des partenaires clés en matière de lutte contre la cybercriminalité comme les États-Unis, le Canada ou l'Australie y sont également parties.

Les motifs de refus figurant aux articles 29, 5., et 30, 2., de la Convention sont mentionnés à l'article 39*quater*, § 2, alinéa 4.

Il est prévu que ces causes de refus de coopération sont "sans préjudice des instruments de droit international liant la Belgique en matière d'entraide judiciaire et tendant à promouvoir celle-ci". Cette formulation est inspirée de l'article 2/3 de la loi du 9 décembre 2004 sur l'entraide judiciaire pénale tel qu'inséré par la loi du 15 mai 2014. L'objectif est d'avoir un cadre évolutif et prendre en compte les normes plus ambitieuses qui pourraient par exemple être établies dans le cadre de l'Union européenne ou sur un plan bilatéral et qui prévoiraient des causes de refus de coopération plus limitées. On peut faire référence à cette même loi pour donner suite à la demande du Conseil d'État de préciser la notion de "intérêts essentiels de la Belgique" (point 21, p. 41 de l'avis). Ces mots sont également utilisés dans cette loi en ce qui concerne les causes de refus d'entraide judiciaire. L'exposé des motifs de cette loi précise à cet égard: "[I]l s'agit, entendue au sens large, de la "clause d'ordre public" telle qu'elle est formulée dans la convention du Conseil de l'Europe sur l'entraide judiciaire en matière pénale de 1959. Cette clause d'ordre public couvre les conflits avec les intérêts de l'État belge (souveraineté, position sur le plan international, ...) ainsi que les cas dans lesquels, notamment en raison de la situation dans l'État requérant, l'exécution est contraire aux principes fondamentaux de la démocratie, de l'État de droit et des droits fondamentaux" (*Doc.parl.* Chambre 2003-04, n° 1278/001, 9).

L'article 29, 7, de la Convention sur la cybercriminalité prévoit un délai de conservation minimum de 60 jours. C'est repris à l'article 39*quater*, § 2, alinéa 6. En cas de demande internationale sur la base de l'article 29 de la Convention sur la cybercriminalité, les données doivent de toute manière être conservées à partir de la réception

ontvangen werd en zolang er geen beslissing is met betrekking tot dit (rechtshulp)verzoek.

Artikel 39*quater*, § 2, 7e lid voorziet in de mogelijkheid om zonder rechtshulp bepaalde data aan een andere natie te overhandigen. Dit om tegemoet te komen aan de situatie waarin wordt vastgesteld dat het op basis van artikel 29 CC aangezochte land eigenlijk maar een "transmissieland "of een "passageland" is.

Meer bepaald is het veelal zo dat het IP-spoor dat de ISP in de aangezochte natie bezit/aanlevert onmiddellijk duidelijk maakt dat de finale identificatie moet geschieden in nog een andere staat. Bijvoorbeeld: België verzoekt Facebook om basic subscriber information veilig te stellen met betrekking tot een welbepaalde facebookaccount. Eigenlijk is al onmiddellijk duidelijk dat de te identificeren "dader" zich niet bevindt in de USA aangezien het IP-adres blijkt toe te behoren aan een ISP of IAP in Nederland. Op dat ogenblik, indien men in de USA vaststelt dat de USA eigenlijk maar een "transmissieland" is, en dat het kennelijk geen data betreft met betrekking tot een US-onderdaan, voorziet de Cybercrimeconventie dat de mogelijkheid moet bestaan om zonder rechtshulpverzoek onmiddellijk de Nederlandse IP vrij te geven, zodat België onmiddellijk zich via een rechtshulpverzoek kan richten tot Nederland voor identificatie van de internaut.

Artikel 5

Artikel 46*bis* van het Wetboek van strafvordering wordt op drie punten aangepast.

Vooreerst wordt het begrip "verstrekker van een elektronische communicatiedienst" vervangen door de omschrijving uit het zogenaamde Yahoo-arrest (arrest Hof van Cassatie van 18/01/2011): "iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden." Daar wordt in het wetsontwerp, om reden van duidelijkheid, het volgende aan toegevoegd: "Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen".

De nieuwe formulering maakt duidelijk dat deze categorie van aanbieders op zeer ruime wijze moet worden geïnterpreteerd. De medewerkingsplicht is dus ook van toepassing op bedrijven die webdiensten aanbieden zoals die van Yahoo Mail, Hotmail, Gmail, etc., maar

de la demande (d'entraide) et tant qu'il n'y a pas de décision quant à cette demande (d'entraide).

L'article 39, § 2, alinéa 7, prévoit la possibilité de remettre certaines données à une autre nation sans demande d'entraide. Ce pour répondre à la situation où il est constaté que sur la base de l'article 29 de la Convention sur la cybercriminalité, le pays requis est en effet un "pays de transmission" ou un "pays de transit".

Plus particulièrement, il est fréquent que la trace IP détenue/fournie par l'ISP dans la nation requise montre immédiatement de manière claire que l'identification finale doit encore intervenir dans un autre État. Par exemple: la Belgique demande à Facebook de mettre en sécurité la "basic subscriber information" concernant un compte Facebook spécifique. En fait, il apparaît immédiatement de manière évidente que l'"auteur" à identifier ne se trouve pas aux États-Unis vu que l'adresse IP semble appartenir à un ISP ou à un IAP aux Pays-Bas. À ce moment, si l'on constate aux États-Unis que les États-Unis ne sont en fait qu'un "pays de transmission", et que les données ne concernent manifestement pas un ressortissant américain, la Convention sur la cybercriminalité prévoit qu'il doit être possible de révéler immédiatement l'IP néerlandaise, sans demande d'entraide judiciaire, de manière à ce que la Belgique puisse directement s'adresser aux Pays-Bas au moyen d'une demande d'entraide afin d'identifier l'internaute.

Article 5

L'article 46*bis* du Code d'instruction criminelle est adapté sur trois points.

D'abord, la notion de "fournisseur d'un service de communications électroniques" est remplacée par la définition prise de l'arrêt Yahoo (arrêt de la Cour de cassation du 18/01/2011): "toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques." Dans un souci de clarté, il y est ajouté dans le projet de loi ce qui suit: "Est également compris le fournisseur d'un service de communications électroniques."

La nouvelle formulation précise que cette catégorie de fournisseurs doit être interprétée au sens très large du terme. L'obligation de coopération s'applique donc également aux entreprises qui proposent des web-services comme Yahoo Mail, Hotmail, Gmail... mais

evengoed op diensten als Facebook, Twitter, WhatsApp, Instagram en alle andere diensten die onder de nieuwe wettelijke omschrijving vallen.

Wegens de lengte van de nieuwe omschrijving was het aangewezen om alle actoren wiens medewerking kan gevorderd worden, op te nemen in een nieuw tweede lid. Ook diende artikel 46*bis* op enkele andere plaatsen aangepast te worden, zodat naar de nieuwe omschrijving in het tweede lid wordt verwezen.

De aanpassing van het begrip "verstrekker van een elektronische communicatiedienst" werd doorgevoerd in alle artikelen van het Wetboek van Strafvordering die deze term hanteren, met dezelfde motivering als hierboven beschreven: naast artikel 46*bis* gaat het om de artikelen 88*bis*, 90*quater*, 464/13 en 464/25.

Ten tweede wordt een wijziging voorzien in het vierde lid van artikel 46*bis*, § 1. Dit lid voorziet ingeval van uiterst dringende noodzakelijkheid in een mondeling akkoord van de procureur des Konings, waarna de officier van gerechtelijke politie de mogelijkheid heeft om mits een schriftelijke beslissing bij de operatoren of dienstenverstrekkers de gegevens bedoeld in het eerste lid op te vorderen.

De maatregel van artikel 46*bis* is zeer laagdrempelig en heden ten dage veelgebruikt. In het licht van de mondelinge mogelijkheden voor de artikelen 88*bis* en 90*ter* van het Wetboek van strafvordering is het onlogisch dat voor deze maatregel een schriftelijke voorafgaande beslissing van een officier van gerechtelijke politie noodzakelijk zou zijn, na mondeling akkoord van de procureur. Het is veel logischer om aan te nemen dat de magistraat zelf een mondelinge beslissing kan nemen die vervolgens wordt uitgevoerd door de politie, waarna de magistraat zo spoedig mogelijk zijn mondelinge beslissing schriftelijk bevestigt.

Overeenkomstig de vorige leden van artikel 46*bis* dient ook de schriftelijke bevestiging gemotiveerd te zijn.

Ten derde verandert het voorontwerp de termijn waarbinnen de medewerking moet worden verleend. Ook wat dit betreft is een gelijkaardige aanpassing doorgevoerd in de artikelen 88*bis*, 90*quater*, 464/13 en 464/25.

Momenteel bepaalt artikel 46*bis*, § 2, eerste lid dat dit moet geschieden "binnen een termijn te bepalen door de Koning, op het voorstel van de minister van Justitie en de minister bevoegd voor Telecommunicatie". Het laatste lid van § 2 bestraft de "weigering" om medewerking te verlenen.

également aux services comme Facebook, Twitter, WhatsApp, Instagram et à tous les autres services qui entrent dans la nouvelle définition légale.

En raison de la longueur de la nouvelle définition, il était indiqué de faire figurer tous les acteurs dont la collaboration peut être requise dans un nouvel alinéa 2. L'article 46*bis* devait lui aussi être adapté à plusieurs autres endroits de manière à renvoyer à la nouvelle définition dans l'alinéa 2.

L'adaptation de la notion de "fournisseur d'un service de communications électroniques" a été effectuée dans tous les articles du Code d'instruction criminelle qui utilisent ces termes, avec la même motivation que celle décrite ci-dessus: outre l'article 46*bis*, sont concernés les articles 88*bis*, 90*quater*, 464/13 et 464/25.

Deuxièmement, une modification est prévue à l'alinéa 4 de l'article 46*bis*, § 1er. Cet alinéa prévoit, en cas d'extrême urgence, un accord verbal du procureur du Roi, l'officier de police judiciaire ayant ensuite la possibilité de requérir, par une décision motivée et écrite, directement ou par l'intermédiaire d'un service de police désigné par le Roi, les données visées à l'alinéa 1er.

La mesure de l'article 46*bis* est très facile à mettre en œuvre et très fréquemment pratiquée de nos jours. A la lumière des possibilités verbales pour les articles 88*bis* et 90*ter* du Code d'instruction criminelles, il n'est pas illogique que, pour cette mesure, une décision écrite préalable d'un officier de la police judiciaire soit nécessaire, après accord verbal du procureur. Il est bien plus logique d'admettre que le magistrat lui-même puisse prendre une décision verbale exécutée ensuite par la police, à la suite de quoi le magistrat confirme dans les plus brefs délais sa décision verbale par écrit.

Conformément aux alinéas précédents de l'article 46*bis*, la confirmation écrite doit elle aussi être motivée.

Troisièmement, l'avant-projet modifie le délai dans lequel cette collaboration doit être apportée.Ici aussi, une adaptation similaire a été effectuée aux articles 88*bis*, 90*quater*, 464/13 et 464/25.

Actuellement, l'article 46*bis*, § 2, alinéa 1er, précise qu'elle doit intervenir "dans un délai à fixer par le Roi, sur la proposition du ministre de la Justice et du ministre compétent pour les Télécommunications". Le dernier alinéa du paragraphe 2 punit le "refus" de prêter son concours.

De genoemde leden worden gewijzigd zodat ze de verplichting opleggen om de gevorderde medewerking te verlenen “in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering”.

Deze toevoeging is nodig om er voor te zorgen dat geen misbruik wordt gemaakt van de situatie door bv. zijn medewerking, al dan niet opzettelijk, blijvend “uit te stellen”, met de argumentatie dat dit niet zou neerkomen op een “weigering” en dus niet strafbaar zou zijn. In werkelijkheid komt dit natuurlijk wél neer op een weigering, waardoor het onderzoek in het gedrang kan komen.

Onder “werkelijke tijd” dient momenteel te worden verstaan, overeenkomstig het KB van 9 januari 2003 houdende modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie: “de minimum tijdsduur nodig voor de uitvoering van een bepaalde prestatie volgens de regels van de kunst, zonder onderbreking en waarvoor aangepaste middelen en personeel werden ingezet*”* (artikel 1, 3.).

De medewerking moet binnen werkelijke tijd worden verleend, tenzij de procureur des Konings in zijn vordering een later tijdstip bepaalt. Ingevolge het advies van de Raad van State (punt 22) wordt het eerste lid van § 2 terminologisch verfijnd. Het is immers niet de termijn waarvoor de modaliteiten vastgelegd worden door de Koning. Deze modaliteiten betreffen de wijze van medewerking voorzien in het hogervermelde KB van 9 januari 2003. Overigens dient verduidelijkt dat de vordering nooit een kortere termijn kan voorzien dan de “werkelijke tijd”. Hetzelfde geldt overigens voor artikel 88*bis*, § 4, eerste lid van het Wetboek van strafvordering (artikel 12 van het ontwerp).

Artikel 6

Artikel 6 verfijnt de wettelijke regeling van de inkijkoperatie. Naast het betreden van een private plaats wordt het mogelijk gemaakt tijdens een inkijkoperatie kennis te nemen van de inhoud van gesloten voorwerpen die zich daar bevinden, zoals bijvoorbeeld slotvaste kasten of safes.

Met “gesloten voorwerp” wordt echter niet een informaticasysteem bedoeld. Om informaticasystemen (zoals laptops of smartphones) te kunnen doorzoeken, is er steeds een bevelschrift van de onderzoekrechter nodig o.g.v. artikel 89*ter* Sv. Nochtans mogen de opsporingsdiensten binnendringen in een informaticasysteem indien dit enkel tot doel heeft een technisch hulpmiddel te plaatsen, te herstellen of terug te nemen in het kader van een observatie (zie verder). Dit is

Les alinéas précités sont modifiés de manière à imposer l’obligation de prêter la collaboration requise “en temps réel ou, le cas échéant, au moment précisé dans la réquisition”.

Cet ajout est nécessaire afin d’éviter tout abus de la situation notamment par le fait d’“ajourner” continuellement sa collaboration technique, de manière intentionnelle ou non, avec l’argumentation que cela ne s’apparenterait pas à un “refus” et que cela ne serait donc pas punissable. En réalité, cela équivaut bien à un refus, susceptible de compromettre l’enquête.

Par “temps réel”, il y a lieu d’entendre actuellement, conformément à l’arrêté royal du 9 janvier 2003 déterminant les modalités de l’obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques, “la durée minimale nécessaire à l’exécution d’une prestation déterminée, selon les règles de l’art, sans interruption et en mettant en œuvre les moyens et le personnel adéquats” (article 1, 3).

La collaboration doit intervenir en temps réel, sauf si le procureur du roi détermine un moment ultérieur dans sa réquisition. Suite à l’avis du Conseil d’État (point 22), l’alinéa 1er du § 2 est affiné sur le plan terminologique. Il ne s’agit en effet pas du délai dans lequel les modalités sont arrêtées par le Roi. Ces modalités concernent le mode de collaboration prévu dans l’AR du 9 janvier 2003 précité. Il y a d’ailleurs lieu de préciser que la réquisition ne peut jamais prévoir un délai plus court que le “temps réel”. Ceci vaut d’ailleurs pour l’article 88*bis*, § 4, alinéa 1er, du Code d’instruction criminelle (article 12 du projet).

Article 6

L’article 6 affine la réglementation légale du contrôle visuel discret. Outre la pénétration dans un lieu privé, il devient possible, lors d’un contrôle visuel discret, de prendre connaissance du contenu des objets fermés qui s’y trouvent, comme des armoires fermées à clé ou des coffres-forts.

Par “objet fermé”, on ne vise toutefois pas un système informatique. Pour pouvoir explorer des systèmes informatiques (comme des laptops ou des smartphones), une ordonnance du juge d’instruction basée sur l’article 89*ter* du Code d’instruction criminelle est toujours requise. Les services de recherche peuvent néanmoins pénétrer dans un système informatique si cela a pour seule finalité de placer, de réparer ou de retirer un moyen technique dans le cadre d’une observation (voir plus

uitdrukkelijk toegelaten in een nieuwe paragraaf 6 van artikel 46*quinquies*.

Dit betreft bijvoorbeeld het gegeven dat de speurders binnendringen in een camerabewakingssysteem dat door de eigenaar is geplaatst, teneinde in werkelijke tijd toegang te krijgen tot de beelden en op die manier de observatie uit te voeren.

Het betreden van een private plaats in het kader van art. 46*quinquies*, § 1 Sv. kan enkel voor de doeleinden die worden bepaald in § 2 van hetzelfde artikel. Dit wetsontwerp breidt deze paragraaf uit zodat het mogelijk wordt de inkijkoperatie te gebruiken voor het herstellen of terugnemen van technische hulpmiddelen in het kader van de observatie.

De finaliteit van deze maatregel, zoals gesteld in § 2, 1° en 2°, van art. 46*quinquies* Sv., is na te gaan of er bewijsmateriaal bestaat, maar niet dit te verzamelen. Er mogen enkel stalen worden genomen, zijnde bewijzen van de aanwezigheid van de zaken bedoeld in § 2, 1°.

Het nemen van een staal is reeds mogelijk. Zoals aangegeven in de memorie van toelichting van de wet van 6 januari 2003 (*Parl. St*. Kamer 50-1688/001, P. 59): "het kan aangewezen zijn dat de politieambtenaren die, naar aanleiding van een inkijkoperatie, een hoeveelheid wit poeder of een hoeveelheid verdachte liquide middelen aantreffen, daar een staal van nemen, teneinde met zekerheid te kunnen bepalen of het hier al dan niet om drugs of hormonenpreparaat gaat."

Deze al bestaande mogelijkheid om stalen te nemen is niet altijd voldoende. De nieuwe paragraaf 5 voorziet dat de onderzoekers een voorwerp gevonden op de plaats van de inkijkoperatie mee te nemen indien het onderzoek van het voorwerp niet ter plaatse kan gebeuren en indien de informatie niet op een andere manier kan worden verkregen. Bij wijze van voorbeeld: in sommige situaties kan het noodzakelijk zijn om te verifiëren of het om hetzelfde wapen gaat dat al gebruikt werd om een misdrijf te plegen. Het wapen moet dan meegenomen kunnen worden voor de tijd die strikt noodzakelijk is voor de ballistische testen. Het bewuste voorwerp dient dan zo spoedig mogelijk teruggeplaatst te worden.

Deze terugplaatsing wordt mogelijk gemaakt door de aanpassing van § 2.

Tot slot voorziet paragraaf 7 dat over het verloop van de inkijkoperatie een proces-verbaal wordt opgemaakt. Wanneer tijdens deze operatie gesloten voorwerpen werden geopend, of voorwerpen werden meegenomen en teruggeplaatst overeenkomstig § 5, dient dit expliciet

loin). Un nouveau paragraphe 6 de l'article 46*quinquies* l'autorise expressément.

Cela concerne par exemple le fait pour les enquêteurs d'entrer dans le système de vidéosurveillance installé par le propriétaire pour avoir accès en temps réel aux images et ainsi réaliser l'observation.

La pénétration dans un lieu privé dans le cadre de l'article 46*quinquies*, § 1er, ne peut avoir lieu qu'aux fins visées au § 2 du même article. Le projet de loi étend ce paragraphe de manière à permettre le recours au contrôle visuel discret pour réparer ou reprendre des moyens techniques dans le cadre de l'observation.

La finalité de cette mesure, précisée au § 2, 1° et 2°, de l'article 46*quinquies* du Code d'instruction criminelle, est de vérifier si des preuves existent mais pas de collecter celles-ci. Seuls des échantillons peuvent être prélevés, à savoir des preuves de la présence des choses visées au § 2, 1°.

La prise d'échantillons est déjà possible. Comme indiqué dans l'exposé des motifs de la Loi du 6 janvier 2003 (*Doc. parl.* Chambre 50-1688/001, p. 59), "il peut être indiqué que les fonctionnaires de police qui, à l'occasion d'un contrôle visuel discret, découvrent une quantité suspecte de poudre blanche ou de substances liquides en prélèvent un échantillon afin de pouvoir déterminer avec certitude s'il s'agit ou non de drogue ou d'une préparation d'hormones".

Cette possibilité déjà existante de prendre des échantillons ne suffit pas toujours. Le § 5 nouveau vise à permettre aux enquêteurs d'emporter un objet trouvé sur les lieux du contrôle visuel discret si l'examen de cet objet ne peut se faire sur place et si l'information ne peut être obtenue d'une autre manière. A titre d'exemple, si une arme à feu est trouvée sur les lieux, il peut s'avérer nécessaire, dans certaines situations, de vérifier si c'est la même arme que celle déjà utilisée pour commettre une infraction. L'arme devrait alors pouvoir être emportée pour la durée strictement nécessaire aux tests balistiques. L'objet en question doit être remis en place dans les plus brefs délais.

L'adaptation du § 2 rend cette remise en place possible.

Enfin, le paragraphe 7 prévoit qu'il est dressé un procès-verbal du déroulement du contrôle visuel discret. Si des objets fermés ont été ouverts pendant cette opération, ou si des objets ont été emportés et replacés conformément au § 5, il doit en être fait explicitement

vermeld te worden. De gebruikte technieken, tactieken, de identiteit van de betrokken personen alsook het exacte tijdstip waarop de inkijkoperatie werd uitgevoerd moeten niet worden opgenomen in het proces-verbaal.

Artikel 7

Dit artikel voert de mogelijkheid in over te gaan tot een infiltratie op internet of een interactie op internet die niet enkel een gerichte verificatie of een arrestatie tot doel heeft.

Aangezien de infiltratie op internet een minder verregaand karakter heeft dan de "klassieke" infiltratie, en aangezien de verschillende contacten gedurende de uitvoering van deze maatregel worden geregistreerd, is een soepeler regime gerechtvaardigd.

De invoering van een specifieke regeling voor infiltratie op internet, naast de infiltratie waarin reeds is voorzien in artikel 47*octies*, is het gevolg van het samenspel van twee aspecten:

— Het eerste aspect is dat de infiltratie die uitsluitend op internet plaatsvindt, minder indringend is, precies omdat zij geen enkel fysiek contact inhoudt. Alleen dat element volstaat niet ter verantwoording van een afzonderlijke regeling omdat, ook al blijft het altijd minder indringend dan een gelijkaardig fysiek contact, de ontwikkeling van internet tot gevolg heeft dat duurzame interacties op internet een aanzienlijke impact kunnen hebben op de persoonlijke levenssfeer van de persoon.

— Het tweede aspect is al even fundamenteel: het betreft het gegeven dat in de infiltratieregeling "internet" erin is voorzien dat alle contacten worden geregistreerd, wat de maatregel a posteriori veel transparanter maakt en de risico's op misbruik voorkomt. Een dergelijke systematische registratie van de contacten is bij infiltratie in de fysieke wereld niet mogelijk omdat zij de integriteit van de infiltrant in gevaar zou brengen.

De eerste paragraaf van artikel 46*sexies* omschrijft de aard en het toepassingsgebied van de interactie of infiltratie op internet.

Het gaat om het onderhouden van contact op het internet door een of meerdere politieambtenaren met een of meerdere personen, al dan niet onder een fictieve identiteit.

Het begrip "internet" moet in ruime zin begrepen worden en omvat onder meer ook het zogenaamde "dark web" (inhoud die bestaat op "*dark nets*" zoals dat van de dienst *Tor*).

mention. Les techniques et tactiques employées, l'identité des personnes impliquées et le moment exact où le contrôle visuel discret a eu lieu ne doivent pas figurer dans le procès-verbal.

Article 7

Cet article introduit la possibilité de procéder à une infiltration ou à une interaction sur Internet qui ne vise pas uniquement une vérification ciblée ou une arrestation.

Étant donné que l'infiltration sur Internet a un caractère moins intrusif que l'infiltration "classique" et que les différents contacts durant l'exécution de cette mesure sont enregistrés, un régime plus souple est justifié.

La création d'un régime spécifique pour l'infiltration Internet par rapport à l'infiltration déjà prévue à l'article 47*octies* résulte de la combinaison de deux aspects:

— Le premier aspect est que l'infiltration qui a lieu exclusivement sur Internet est moins intrusive précisément parce qu'elle n'implique aucun contact physique. Cet élément seul ne suffit pas à justifier un régime distinct dans la mesure où, même si cela restera toujours moins intrusif qu'un contact physique correspondant, le développement d'Internet fait que des interactions durables sur Internet peuvent avoir un impact majeur sur la vie privée de la personne.

— Le deuxième aspect est tout aussi fondamental: il s'agit du fait que, dans le régime de l'infiltration "Internet", il est prévu que tous les contacts soient enregistrés ce qui rend la mesure beaucoup plus transparente a posteriori et évite les risques d'abus. Un tel enregistrement systématique des contacts dans l'infiltration dans le monde physique n'est pas possible car elle mettrait l'intégrité de l'infiltrant en danger.

Le premier paragraphe de l'article 46*sexies* définit la nature et le champ d'application de l'interaction ou de l'infiltration sur Internet.

Il s'agit pour un ou plusieurs fonctionnaires de police d'entretenir des contacts sur Internet avec une ou plusieurs personnes, sous une identité fictive ou non.

La notion d'"Internet" doit être comprise au sens large et comprend notamment le "dark web" (contenu qui existe sur des "*dark nets*" comme celui du service *Tor*).

Concrete voorbeelden:

— De politie beschikt over ernstige aanwijzingen dat een bepaalde persoon online een handel heeft opgezet in verboden vuurwapens, drugs of kinderpornografie. De procureur des Konings kan een infiltratie op internet bevelen om de persoon en eventuele mededaders verder te identificeren, om bewijsmateriaal te verzamen en dergelijke meer;

— Inzake het fenomeen "*grooming*": Een verontruste ouder meldt dat zijn of haar minderjarige dochter op een sociaal netwerk door een man werd benaderd met de duidelijke bedoeling haar seksuele handelingen te laten stellen en zelfs aanstuurde met haar af te spreken. Het sociale netwerk laat geen exacte lokalisatie van het profiel toe en gebruikers kunnen deze optie uitzetten. Bovendien is deze GPS-locatie enkel actief in de community voor volwassenen. Door als politiedienst onder een fictieve identiteit een profiel aan te maken en zich op dit sociaal netwerk te begeven, kan in een eerste fase al geprobeerd worden het bestaan van het geviseerde profiel te achterhalen. Het fictieve profiel aangemaakt door de politie kan zodanig opgemaakt worden (zonder expliciet, misleidend of provocatief te zijn) dat dit mogelijks de aandacht van de kinderlokker trekt en hij hiermee contact zoekt. Dankzij de mogelijkheid van artikel 46*sexies* kan de politieman die dit profiel beheert, proberen meer informatie van de kinderlokker te verkrijgen om hem uiteindelijk te identificeren, en eventueel met hem afspreken om elkaar te ontmoeten op een publieke plaats waar hij dan kan onderschept worden.

Bij de uitvoering van deze maatregel mogen de opsporingsdiensten zich uiteraard niet schuldig maken aan provocatie (artikel 30 van de Voorafgaande Titel van het Wetboek van Strafvordering).

De maatregel kan enkel worden bevolen wanneer het een onderzoek naar misdaden of wanbedrijven betreft. Verder moet aan de subsidiariteitsvereiste voldaan zijn, die identiek is geformuleerd als bij de "klassieke" infiltratie van artikel 47*octies* Sv. Tenslotte moet de machtigende magistraat over ernstige aanwijzingen beschikken dat de geviseerde personen misdrijven plegen of zouden plegen die bestraft worden met een gevangenisstraf van een jaar of een zwaardere straf. Dit is dezelfde proportionaliteitsdrempel als deze die is voorzien voor de observatie met technische hulpmiddelen (artikel 47*sexies*, § 2, tweede lid Sv.).

Het derde lid van de eerste paragraaf laat toe dat bij de uitvoering van de maatregel, in uitzonderlijke omstandigheden en kortstondig, beroep wordt gedaan

Exemples concrets:

— La police dispose d'indices sérieux indiquant qu'une certaine personne a mis sur pied un trafic en ligne d'armes à feu prohibées, de drogue ou de pornographie enfantine. Le procureur du roi peut ordonner une infiltration sur Internet afin d'identifier la personne et d'éventuels coauteurs, de collecter des preuves, etc.

— Concernant le phénomène de "*grooming*": Un parent inquiet signale que sa fille mineure a été approchée sur un réseau social par un homme dans le but manifeste de lui faire poser des actes à caractère sexuel et qu'il a même essayé de lui fixer rendez-vous. Le réseau social ne permet pas d'obtenir la localisation exacte du profil et les utilisateurs peuvent décocher cette option. Par ailleurs, cette localisation GPS n'est active dans la communauté que pour les adultes. Autoriser le service de police à créer un profil sous une identité fictive et à aller sur ce réseau social permet dans une première phase de déjà tenter de retracer la présence du profil visé. Le profil fictif créé par la police peut être établi (sans être explicite, trompeur ou provocant) de manière à éventuellement attirer l'attention du pédophile et à l'amener à prendre contact. Grâce à la possibilité prévue à l'article 46*sexies*, le policier qui gère ce profil peut essayer d'obtenir davantage d'informations sur le pédophile pour finalement l'identifier et convenir éventuellement avec lui d'un rendez-vous dans un lieu public où il pourra alors être intercepté.

Dans le cadre de l'exécution de cette mesure, les services de recherche ne peuvent évidemment pas se rendre coupables de provocation (article 30 du Titre préliminaire du Code de procédure pénale).

La mesure ne peut être ordonnée que lorsqu'elle concerne une enquête sur des crimes ou des délits. En outre, la condition de subsidiarité, formulée de la même manière que dans l'infiltration "classique" de l'article 47*octies* du Code d'instruction criminelle, doit être remplie. Enfin, le magistrat qui délivre l'autorisation doit disposer d'indices sérieux indiquant que les personnes visées commettent ou commettraient des infractions punissables d'un emprisonnement d'un an ou d'une peine plus lourde. Le seuil de proportionnalité est le même que celui prévu pour l'observation effectuée à l'aide de moyens techniques (article 47*sexies*, § 2, alinéa 2, du Code d'instruction criminelle).

Le troisième alinéa du premier paragraphe permet de faire appel, dans des circonstances exceptionnelles et pour une courte durée, à un expert civil dans le cadre

op een burgerdeskundige. Dit betekent niet dat de uitvoering van de maatregel aan deze persoon mag worden gedelegeerd.

Concrete voorbeelden:

— Indien agenten zich begeven in milieus waar een specifieke taal (vreemde taal, jongerentaal,…) gehanteerd wordt, kunnen zij zich laten bijstaan door een taaldeskundige;

— In sommige milieus is zeer specialistische kennis vereist: zo kan het in een hackersmilieu noodzakelijk zijn dat een beroep wordt gedaan op een specialist die over de nodige hoogtechnologische kennis beschikt.

Het vierde lid verduidelijkt dat artikel 46*sexies* geen toepassing vindt wanneer politieambtenaren overgaan tot een persoonlijke interactie op internet die slechts een gerichte verificatie of een arrestatie tot direct doel heeft. In die gevallen is dan ook geen voorafgaande machtiging van de procureur des Konings vereist.

Die verduidelijking strekt ertoe te voorkomen dat een situatie wordt gecreëerd waarin de slagvaardigheid van de politiediensten wordt beperkt ten opzichte van wat thans bestaat, zowel op internet als in de fysieke wereld.

— Persoonlijke interactie die enkel een gerichte verificatie tot direct doel heeft

In het kader van hun opdracht inzake de opsporing van strafbare feiten baseren de politiediensten zich bijvoorbeeld op de in de kranten gepubliceerde “zoekertjes” voor de opsporing van verdachte verkopen (van gsm’s of gestolen wagens bijvoorbeeld). Zij kunnen dan het vermelde nummer opbellen om een afspraak te maken en het betrokken goed te controleren, zonder een fictieve identiteit aan te nemen, maar ook zonder erop te wijzen dat zij politieambtenaar zijn. In internettijden is het equivalent bijvoorbeeld dat het betrokken voorwerp wordt opgespoord op een tweedehandsverkoopsite en dat via die site een e-mail wordt gestuurd naar de verkoper om een afspraak te maken en het betrokken goed te zien.

Ook bij het analyseren van dreigende berichten op internet kan een gerichte verificatie nodig zijn. Een korte persoonlijke interactie met de persoon die het bericht geplaatst heeft, kan al uitwijzen of deze een “echte” radicaal/terrorist/… is, dan wel een flauwe grappenmaker of een fantast.

de l’exécution de la mesure. Cela ne signifie pas que l’exécution de la mesure puisse être déléguée à cette personne.

Exemples concrets:

— Si des agents pénètrent dans des milieux où est utilisé un langage spécifique (langue étrangère, langage de jeunes...), ils peuvent se faire assister par un expert en langue;

— Dans certains milieux, des connaissances très spécialisées sont requises: ainsi, il peut être nécessaire dans un milieu de hackers de faire appel à un spécialiste qui possède les connaissances nécessaires en matière de haute technologie.

Le quatrième alinéa précise que l’article 46*sexies* n’est pas d’application lorsque les fonctionnaires de police procèdent à une interaction personnelle sur Internet dont la finalité directe est uniquement une vérification ciblée ou une arrestation. Dans ces cas, aucune autorisation préalable du procureur du Roi n’est dès lors requise.

Cette précision vise à éviter de créer une situation où les services de police voient leur capacité d’action sur Internet réduite par rapport à ce qui existe actuellement que ce soit sur Internet ou dans le monde physique.

— Interaction personnelle ayant pour seule finalité directe une vérification ciblée

Par exemple, dans le cadre de leur mission de détection des infractions pénales, les services de police se basent sur les “petites annonces” publiées dans les journaux pour repérer des mises en vente suspectes (GSM ou voiture volés par ex.). Ils peuvent alors appeler le numéro indiqué pour prendre un rendez-vous et vérifier le bien en question, sans prendre d’identité fictive mais sans non plus indiquer leur qualité de policier. A l’heure d’Internet, l’équivalent est par exemple de repérer l’objet concerné sur un site de vente d’occasion et d’envoyer un email au vendeur via ce site pour prendre rendez-vous et voir le bien en question. Ce type d’action ne nécessite pas l’accord préalable du magistrat et le régime prévu par le nouvel article 46*sexies*.

Une vérification ciblée peut également être nécessaire dans le cadre de l’analyse de messages de menace sur Internet. Une brève interaction personnelle avec la personne qui a posté le message permet déjà de déterminer s’il s’agit d’un “véritable” radical/terroriste/..., d’un malheureux plaisantin ou d’un fabulateur.

Deze voorbeelden worden beschouwd als persoonlijke interacties die enkel een gerichte verificatie tot direct doel hebben. Voor dat soort acties zijn het voorafgaand akkoord van de magistraat en de regeling waarin het nieuwe artikel 46*sexies* voorziet, dan ook niet vereist.

— Persoonlijke interactie die enkel een arrestatie tot direct doel heeft

Een interactie op internet die enkel een arrestatie tot direct doel heeft, is bijvoorbeeld een gerichte interactie waarbij een politieambtenaar onder valse voorwendselen met een internetgebruiker afspreekt om elkaar fysiek te ontmoeten, teneinde deze persoon te kunnen arresteren.

De arrestatie moet een doelstelling op korte termijn ("direct doel") zijn. Persoonlijke interacties die bijvoorbeeld dienen om bewijsmateriaal te verzamelen en die pas nadien tot een arrestatie moeten leiden, worden dus niet geviseerd.

De arrestatie moet uiteraard rechtmatig zijn. Artikel 46*sexies*, § 1, vierde lid verschaft geen nieuwe rechtsbasis voor de arrestatie van een verdachte.

Bij persoonlijke interacties die een gerichte verificatie of arrestatie tot direct doel hebben, mag geen geloofwaardige fictieve identiteit gebruikt worden.

In haar advies over dit ontwerp van wet stelt de Privacycommissie vragen bij die verwijzing naar de interactie die een gerichte verificatie of een arrestatie tot direct doel heeft. Zij vestigt de aandacht op haar advies nr. 13/2015 waarin zij zich heeft gebogen over een ontwerp van wijziging van artikel 26 van de wet op het politieambt, met de bedoeling in de wet nader te bepalen wat de politie op het internet mag doen in het kader van haar taken van bestuurlijke politie en in het kader van haar taken van gerechtelijke politie. Wat de taken van gerechtelijke politie betreft, heeft artikel 26 betrekking op de bevoegdheden van de politie vóór de opening van het strafrechtelijk onderzoek, inzonderheid in het kader van de opdracht inzake de opsporing van strafbare feiten.

Op het stuk van de interactie op het internet die enkel een gerichte verificatie of een arrestatie tot doel heeft, heeft de verduidelijking die in dit ontwerp van wet wordt verschaft enkel betrekking op een specifiek en zeer beperkt aspect. Het is enkel de bedoeling (doel)gerichte contacten toe te staan met een verificatie of arrestatie als specifiek en direct doel. Het is niet de bedoeling vooruit te lopen op het debat over artikel 26 van de wet op het politieambt wat het optreden van de politie op het internet betreft. De discussies over dat aspect van

Ces exemples sont considérés comme des interactions personnelles qui ont pour seule finalité directe une vérification ciblée. Ce type d'actions ne nécessite dès lors pas l'accord préalable du magistrat et l'ordonnance prévue au nouvel article 46*sexies*.

— Interaction personnelle ayant pour seule finalité directe une arrestation

Une interaction sur Internet qui a pour seule finalité directe une arrestation est par exemple une interaction ciblée dans le cadre de laquelle un fonctionnaire de police se met d'accord avec un utilisateur d'Internet pour une rencontre physique, sous de faux prétextes, afin de pouvoir arrêter cette personne.

L'arrestation doit être un objectif à court terme ("finalité directe"). Des interactions personnelles qui servent, par exemple, à collecter des éléments de preuve et qui ne doivent conduire qu'ensuite à une arrestation ne sont donc pas visées.

L'arrestation doit évidemment être légitime. L'article 46*sexies*, § 1, alinéa quatre ne fournit pas une nouvelle base juridique pour l'arrestation d'un suspect.

Le recours à une identité fictive crédible n'est pas autorisé pour des interactions personnelles qui ont pour finalité directe une vérification ou une arrestation ciblée.

Dans son avis sur le présent projet de loi, la Commission vie privée s'interroge sur cette référence à l'interaction aux fins directes de vérification ciblée ou d'arrestation. Elle rappelle son avis n° 13/2015 dans lequel elle s'est penchée sur un projet de modification de l'art. 26 de la Loi sur la fonction de police visant à préciser dans la loi ce que la police peut faire en police administrative et en police judiciaire sur Internet. S'agissant de la police judiciaire, l'art. 26 concerne les pouvoirs de la police en amont de l'ouverture de l'enquête pénale, notamment dans le cadre de la mission de détection des infractions pénales.

La précision apportée dans le présent projet de loi s'agissant de l'interaction sur Internet visant seulement la vérification ciblée ou l'arrestation ne vise qu'un aspect spécifique et très limité. Il s'agit seulement de permettre des contacts ponctuels et ciblés dans un but précis et direct de vérification ou d'arrestation. Il ne s'agit pas d'anticiper sur le débat sur l'article 26 de la Loi sur la fonction de police s'agissant de l'action de la police sur Internet. Les discussions sur cet aspect de l'article 26 de la Loi sur la fonction de police se poursuivent au

artikel 26 van de wet op het politieambt worden verder gevoerd binnen de regering. Die discussies hebben niet alleen betrekking op de taken van gerechtelijke politie maar ook over de taken van bestuurlijke politie en dit ontwerp van wet was dan ook niet het passende instrument om dat vraagstuk op te lossen.

Voor de duidelijkheid en ten gevolge van voormelde opmerking van de Privacycommissie, maakt paragraaf 1, vierde lid nu gewag van "opdrachten van gerechtelijke politie". Hiermee wordt duidelijk gemaakt dat het wetsontwerp geen impact heeft op de bestuurlijke politie en dat het in geen geval kan worden geïnterpreteerd als een definitie van de bevoegdheden in het kader van de opdrachten van bestuurlijke politie.

Wat betreft de politiediensten die de nieuwe maatregel zullen kunnen uitvoeren, is het niet noodzakelijk om een even strikte regeling te hebben als de thans bestaande regeling voor de infiltratie. Die laatste is voorbehouden voor de leden van de speciale eenheden van de federale politie (DSU). Dat is verantwoord op grond van het gevaar dat de maatregel inhoudt, ook en vooral voor de infiltrerende politieambtenaar. Die beperking is niet verantwoord voor de maatregel die uitsluitend op internet plaatsvindt. Dat betekent evenwel niet dat om het even welke onderzoeker kan worden belast met de uitvoering van een dergelijke interactie of infiltratie. Enkel de specifiek aangewezen politiediensten zullen de maatregel kunnen uitvoeren. In het voorontwerp werd deze aanwijzing gedelegeerd aan de minister van Justitie. De Raad van State merkt op dat een dergelijke delegatie niet toegestaan is en dat de bevoegde politiediensten in de wet zouden moeten worden opgenomen. De regering wijst er op dat een delegatie aan de minister van Justitie reeds bestaat in het raam van de toepassing van bijzondere opsporingsmethoden (art. 47*ter*, § 1, tweede lid Sv.) en dat het niet aan de wetgever toekomt om een gedetailleerde regeling uit te werken. Er zal immers worden voorzien in een specifieke opleiding voor de beoogde politiediensten met het oog op zowel de bescherming van de persoonlijke levenssfeer van de beoogde personen als het verzekeren van het goede verloop van de onderzoeken. Om die reden opteert de regering ervoor om de voorwaarden, onder meer wat betreft de opleiding, en modaliteiten van de aanwijzing van de bevoegde politiediensten door de Koning te laten bepalen.

De tweede paragraaf schrijft voor dat de machtiging tot interactie of infiltratie op internet steeds schriftelijk en gemotiveerd moet zijn. In spoedeisende gevallen, waarin een voorafgaande machtiging niet mogelijk is, moet een mondelinge machtiging worden bekomen die nadien schriftelijk en gemotiveerd moet worden bevestigd.

sein du gouvernement. Ces discussions ne concernent pas seulement la police judiciaire mais aussi la police administrative et le présent projet de loi n'était donc pas l'instrument adéquat pour régler cette question.

Pour être clair et suite à la remarque de la Commission vie privée, le paragraphe 1, alinéa 4 mentionne actuellement les "missions de police judiciaire". Il est ainsi clarifié que le projet de loi n'a pas d'impact sur la police administrative et qu'il ne peut nullement être compris comme une définition des compétences dans le cadre des missions de police administrative.

S'agissant des services de police qui vont pouvoir réaliser la nouvelle mesure, il n'est pas nécessaire d'avoir un régime aussi strict que pour l'infiltration telle qu'elle existe actuellement. Cette dernière est réservée aux membres des unités spéciales de la police fédérale (DSU). Cela est justifié par la dangerosité de la mesure, y compris et surtout pour l'agent infiltrant. Cette limitation n'est pas justifiée pour la mesure se déroulant exclusivement sur Internet. Cela ne signifie toutefois pas que tout enquêteur pourra se voir charger d'exécuter une telle interaction ou infiltration. Seuls les services de police spécifiquement désignés pourront exécuter la mesure. Une formation spécifique sera prévue tant pour protéger la vie privée des personnes visées que pour assurer le bon déroulement des enquêtes. Dans l'avant-projet, cette désignation était déléguée au ministre de la Justice. Le Conseil d'État observe qu'une telle délégation n'est pas autorisée et que les services de police compétents devraient être repris dans la loi. Le gouvernement fait remarquer qu'une telle délégation au ministre de la Justice existe déjà dans le cadre de l'application des méthodes particulières de recherche (art. 47*ter*, § 1er, alinéa 2, CIC) et qu'il n'appartient pas au législateur d'élaborer un règlement détaillé. Une formation spécifique sera en effet prévue pour les services de police visés, en vue aussi bien de la protection de la vie privée des personnes visées que de l'assurance du bon déroulement des enquêtes. Pour ces raisons, le gouvernement prend l'option de faire déterminer les conditions, y compris pour ce qui concerne la formation, et modalités de la désignation des services de police compétents par le Roi.

Le deuxième paragraphe prescrit que l'autorisation d'interaction ou d'infiltration sur Internet doit toujours être formulée par écrit et motivée. En cas d'urgence, quand une autorisation préalable n'est pas possible, une autorisation verbale doit être obtenue, laquelle sera ensuite confirmée par écrit et motivée.

De machtiging tot infiltratie op internet is geldig voor een periode van maximaal drie maanden. Verlenging is mogelijk, indien nog steeds voldaan is aan de voorwaarden van de eerste paragraaf.

Dat de schriftelijke machtiging van de procureur des Konings met reden omkleed moet zijn, houdt in dat hij expliciet moet motiveren dat aan de voorwaarden van de eerste paragraaf is voldaan, namelijk de subsidiariteit en de ernstige aanwijzingen van strafbare feiten waarop minstens één jaar gevangenisstraf staat.

De derde paragraaf van artikel 46*sexies* beoogt een regeling uit te werken die het plegen van strafbare feiten door politieambtenaren toelaat. Deze regeling is gelijkaardig aan deze van artikel 47*quinquies*, zodat kan worden verwezen naar de toelichting bij dit artikel (zie Memorie van Toelichting bij de wet van 6 januari 2003, *Parl.St.* Kamer 2001-02, nr. 1688/001, 70-72).

Voorbeelden van strafbare feiten die gemachtigd kunnen worden:

— Berichten sturen of posten op een forum van radicalen/extremisten, waarbij de holocaust ontkend wordt, racistische uitlatingen gedaan worden, gedreigd wordt tot het plegen van een aanslag,…;

— Technieken gebruiken aan de hand waarvan de verdachte gelokaliseerd kan worden;

— De uitwisseling van illegale bestanden via private peer-to-peer netwerken. Hierbij plaatsen gebruikers in hun profiel bepaalde bestanden, die dan door andere, “bevriende” gebruikers gedownload kunnen worden.

De beslissingen waarbij het plegen van strafbare feiten wordt toegelaten of waarbij het beroep op een burgerdeskundige wordt gemachtigd, worden bewaard in een vertrouwelijk dossier dat onderhevig is aan controle door de kamer van inbeschuldigingstelling. Er moet evenwel worden benadrukt dat er niet in ieder geval een vertrouwelijk dossier zal moeten worden opgemaakt. Dit zou de procedure enorm verzwaren, gelet op de verplichte wettigheidscontrole door de kamer van inbeschuldigingstelling. Enkel als de procureur des Konings misdrijven machtigt of een burgerdeskundige inschakelt, moet hij een vertrouwelijk dossier aanleggen. Een omzendbrief van het College van procureurs-generaal kan nadere richtlijnen vastleggen aangaande de situaties waarin de machtiging van misdrijven of de inschakeling van een burgerdeskundige aangewezen is.

De Raad van State heeft in haar advies verwezen naar advies 32 673/2 met betrekking tot artikel

L’autorisation d’infiltration sur Internet est valable pour une période de trois mois maximum. Une prolongation est possible si les conditions du premier paragraphe sont toujours remplies.

Le fait que l’autorisation du procureur du Roi doive être motivée implique qu’il doit explicitement motiver le fait que les conditions du premier paragraphe sont remplies, à savoir la subsidiarité et les indices sérieux de l’existence d’infractions punissables d’un emprisonnement d’au moins un an.

Le troisième paragraphe de l’article 46*sexies* vise l’élaboration d’une réglementation permettant la commission d’infractions par des fonctionnaires de police. Cette réglementation est similaire à celle de l’article 47*quinquies*, de sorte qu’il peut être renvoyé au commentaire de cet article (voir exposé des motifs de la loi du 6 janvier 2003, *Doc. parl.*, Chambre, 2001-02, n° 1688/001, 70-72).

Exemples d’infractions qui peuvent être autorisées:

— Envoyer ou poster des messages sur un forum de radicaux/extrémistes sur lequel on nie l’holocauste, on fait des déclarations racistes, on menace de commettre un attentat...;

— Utiliser des techniques à l’aide desquelles le suspect peut être localisé;

— Échanger des fichiers illégaux via des réseaux privés ou peer-to-peer. Ici, des utilisateurs placent dans leur profil certains fichiers qui peuvent être téléchargés par d’autres utilisateurs “amis”.

Les décisions autorisant la commission d’infractions ou le recours à un expert civil sont conservées dans un dossier confidentiel soumis à un contrôle de la chambre des mises en accusation. Il convient toutefois de souligner qu’un dossier confidentiel ne devra pas être établi dans tous les cas. Cela alourdirait énormément la procédure, vu le contrôle de la légalité obligatoire de la chambre des mises en accusation. Ce n’est que si le procureur du Roi autorise des infractions ou fait appel à un expert civil qu’il devra constituer un dossier confidentiel. Une circulaire du Collège des procureurs généraux peut fixer des directives plus précises concernant les situations où l’autorisation d’infractions ou le recours à un expert civil est indiqué.

Dans son avis, le Conseil d’État réfère à l’avis 32 673/2 en ce qui concerne l’article 47*quinquies* du

47*quinquies* van het Wetboek van Strafvordering. De Raad herhaalt dat bepaalde misdrijven uitgesloten zouden moeten worden, en dat er een onderscheid gemaakt zou moeten worden tussen de politieinfiltrant en de burgermedewerker. De regering wenst in eerste instantie te verwijzen naar de Memorie van Toelichting bij de wet van 6 januari 2003 (*Parl.St.* Kamer 2001-02, nr. 1688/001, 70-72), waarin ook al ingegaan wordt op deze bedenkingen van de Raad van State. Daar kan nog aan toegevoegd worden dat het tweede lid van § 3 voldoende garantie biedt door te stellen dat de strafbare feiten niet ernstiger mogen zijn dan die waarvoor de maatregel wordt aangewend.

De Raad van State vraagt zich in punt 25 van het advies ook af waarom de procureur des Konings, in tegenstelling tot wat het geval is voor de klassieke infiltratie, geen maatregelen kan nemen ter vrijwaring van de veiligheid en de fysieke, psychische en morele integriteit van de cyberinfiltrant (zie artikel 47*octies*, § 2 laatste lid). De regering acht dit overbodig bij een infiltratie die enkel via internet verloopt. Er is vooreerst geen enkel fysiek contact met mogelijke verdachten. Bovendien spreekt het voor zich dat de cyber-infiltranten voortdurend zullen worden opgevolgd. Voor het garanderen van hun psychologische en morele integriteit is geen wettelijke basis vereist.

De Raad van State vraagt waarom de toegelaten strafbare feiten niet beperkt worden tot cyberspace. De regering acht het beperken van de strafbare feiten echter niet wenselijk. Er kan bijvoorbeeld gedacht worden aan het opmaken van een vals document dat vervolgens ingescand wordt en doorgestuurd naar de verdachte. Dit is een strafbaar feit dat zich niet in cyberspace heeft voorgedaan, maar wel voorafgaand aan het contact met de verdachte.

In punt 29 van haar advies meent de Raad van State dat artikel 46*sexies*, § 3, zesde lid de voorafgaande controle van de procureur des Konings uitholt. De regering is van mening dat dit niet het geval is. Vooreerst is de gehele regeling omtrent het plegen van misdrijven door politieambtenaren quasi identiek aan de regeling die vandaag reeds geldt bij toepassing van de bijzondere opsporingsmethoden (artikel 47*quinquies* Sv.). Het voorzien van de mogelijkheid om strafbare feiten te plegen zonder voorafgaande machtiging van de procureur des Konings is in dezelfde mate noodzakelijk als bij de klassieke infiltratie. De memorie van toelichting bij de "BOM-wet" van 6 januari 2003 motiveert dit als volgt:

"Het kan niet worden uitgesloten dat de politieambtenaar, tijdens de uitvoering van de bijzondere opsporingsmethoden, geconfronteerd wordt met uitzonderlijke

Code d'instruction criminelle. Il répète que certaines infractions devraient être exclues et qu'il faudrait opérer une distinction entre le policier infiltrant et le collaborateur civil. Le gouvernement souhaite en première instance référer à l'Exposé des motifs de la loi du 6 janvier 2003 (*Doc. parl.*, Chambre, 2001-2002, n° 1688/001, 70-72), où il est déjà donné suite à ces considérations du Conseil d'État. On peut y ajouter que l'alinéa 2 du paragraphe 3 offre une garantie suffisante pour dire que les faits punissables ne peuvent pas être plus graves que ceux pour lesquels la mesure est utilisée.

Le Conseil d'État se demande aussi, au point 25 de l'avis, pourquoi le procureur du Roi, contrairement à ce qui est le cas pour l'infiltration classique, ne peut pas prendre des mesures en vue de garantir la sécurité, ainsi que l'intégrité physique, psychique et morale du cyberinfiltrant (voir l'article 47*octies*, § 2, dernier alinéa, du Code d'instruction criminelle). Le gouvernement estime que ceci est superflu lorsqu'une infiltration est réalisée uniquement via Internet. Il n'y a tout d'abord pas de contact physique avec d'éventuels suspects. En outre, il va de soi que les cyberinfiltrants continueront de faire l'objet d'un suivi. Aucune base légale n'est requise pour garantir leur intégrité psychique et morale.

Le Conseil d'État demande pourquoi les faits punissables autorisés ne sont pas limités au cyberespace. Le gouvernement estime toutefois que la limitation des faits punissables n'est pas souhaitable. On peut songer, par exemple, à l'établissement d'un faux document qui est ensuite scannée et transmis au suspect. Il s'agit d'un fait punissable qui n'est pas survenu dans le cyberespace mais bien préalablement au contact avec le suspect.

Au point 29 de son avis, le Conseil d'État considère que l'article 46*sexies*, § 3, alinéa 6, vide le contrôle préalable du procureur du Roi de sa substance. Le gouvernement est d'avis que cela n'est pas le cas. Tout d'abord, l'ensemble du règlement concernant la commission d'infractions par des fonctionnaires de police est quasiment identique à celui qui, de nos jours, s'applique déjà lors du recours aux méthodes particulières de recherche (article 47*quinquies*, CIC). Prévoir la possibilité de commettre des faits punissables sans autorisation préalable du procureur du Roi est nécessaire dans la même mesure que lors de l'infiltration classique. L'exposé des motifs de la "loi-BOM" du 6 janvier 2003 motive ceci comme suit:

"Il ne peut être exclu qu'un fonctionnaire de police soit confronté, lors de l'exécution des méthodes particulières de recherche, à des circonstances exceptionnelles qui

omstandigheden, die hem er toe nopen strafbare handelingen te stellen, die niet te voorzien waren en niet op voorhand met de magistraat konden worden doorgesproken. In sommige gevallen bestaat nog de mogelijkheid om, alvorens de strafbare feiten daadwerkelijk te stellen, mondeling de magistraat in kennis te stellen. In andere gevallen is zelfs dit onmogelijk.

Wederom kan gedacht worden aan de infiltrant. Bij infiltratie is niet steeds te voorzien welke handelingen nodig zullen zijn, wil de infiltrant zich ten behoeve van zijn opdracht geloofwaardig maken als deelnemer aan een criminele organisatie. Zijn veiligheid kan op het spel staan, als hij (onverwachte) opdrachten weigert die een deelnemer in de organisatie in zijn positie niet behoort te weigeren (…) Het volstaat dat hij onverwacht door de criminele organisatie wordt uitgenodigd een verdachte transactie of een strafbaar feit daadwerkelijk zelf bij te wonen, opdat hij zich in een positie van potentieel mededaderschap of medeplichtigheid aan misdrijven bevindt. In dergelijke gevallen is het onvermijdbaar dat de politieambtenaar strafbare feiten pleegt" (*Parl St.* Kamer 2001-2002, 50-1688/001, 26)."

Bovendien behoudt de procureur des Konings steeds zijn recht om het gepleegde misdrijf a posteriori te toetsen:

"Het komt de magistraat dan toe, weliswaar achteraf, een oordeel te vellen over de handelingen en gedragingen van de politieambtenaar en deze af te toetsen aan de situatie, zoals zij zich heeft voorgedaan en waarin de politieambtenaar, soms in een fractie van tijd, tot het nemen van een beslissing werd gedwongen. Ook hier zal de magistraat de gepleegde strafbare feiten beoordelen in het licht van het welslagen van de operatie en de veiligheid van de politieambtenaar of andere bij de operatie betrokken personen. Mocht de magistraat van oordeel zijn dat de gepleegde strafbare feiten het kader van de opdracht of van de bijzondere opsporingsmethoden volledig te buiten gaan of werkelijk onrechtmatig en onaanvaardbaar zijn, zal hij hieraan het strafrechtelijk gevolg, dat hij passend acht, verlenen."(*Parl. St.* Kamer 2001-2002, 50-1688/001, p. 26-27)."

Tot slot meent de Raad van State dat de laatste zin van artikel 46*sexies*, § 3, zevende lid, waarin gesteld wordt dat het vertrouwelijk dossier onder het beroepsgeheim valt, kan weggelaten worden omdat dit een evidentie is. De regering wenst echter de overeenkomst met het huidige recht te behouden en verwijst naar de andere artikelen omtrent het vertrouwelijk dossier, die

le contraignent à commettre des actes punissables qui n'étaient pas prévus et qui n'ont donc pas fait l'objet d'une étroite concertation avec le magistrat compétent. Dans certains cas, il est possible, avant la perpétration effective des infractions, d'en informer oralement le magistrat. Dans d'autres, cela n'est même pas possible.

A cet égard, on peut de nouveau prendre l'infiltrant comme exemple. Lors d'une infiltration, il n'est pas toujours possible de prévoir quels actes l'infiltrant devra commettre comme participant à l'organisation criminelle pour se rendre crédible en vue de garantir sa mission. Sa sécurité peut être en danger s'il refuse des missions (imprévues) qu'un membre de l'organisation, à son échelon, ne devrait pas refuser, par exemple, être présent lors d'une affaire de trafic de drogue, le recel de marchandises volées, la participation à la préparation d'un transport illégal, etc. Il suffit qu'il soit subitement invité par l'organisation criminelle à assister à une transaction suspecte ou à un fait effectivement punissable pour qu'il se trouve en position de coauteur ou de complice potentiel d'infractions. Dans ces cas, le fonctionnaire de police ne peut pas faire autrement que commettre des infractions." *(Doc. parl.,* Chambre 2001-2002, 50-1688/001, p. 26).

En outre, le procureur conserve toujours son droit d'évaluer *a posteriori* l'infraction commise:

"Il appartient alors au magistrat de rendre un jugement, a posteriori bien évidemment, sur les actes et comportements du fonctionnaire de police et de les évaluer au regard de la situation telle qu'elle s'est présentée et dans laquelle le fonctionnaire de police, parfois en une fraction de seconde, a dû prendre une décision. Le magistrat jugera les infractions commises à la lumière de la réussite de l'opération et de la protection et de la sécurité du fonctionnaire de police ou des autres personnes impliquées dans l'opération. Si le magistrat est d'avis que les infractions commises sortent complètement du cadre de la mission ou que ceux-ci sont injustifiables ou inacceptables, il leur donnera la suite pénale qu'il estime opportune." (*Doc. parl.*, Chambre 2001-2002, 50-1688/001, p. 26-27).

Enfin, le Conseil d'État est d'avis que la dernière phrase de l'article 46*sexies*, § 3, alinéa 7, qui dispose que le contenu du dossier confidentiel est couvert par le secret professionnel, peut être omise parce qu'elle ne fait que traduire une évidence. Le gouvernement souhaite toutefois maintenir la correspondance avec le droit actuel et réfère aux autres articles relatifs au

deze zin ook vermelden. Het weglaten van deze zin zou dan tot een redenering *a contrario* kunnen leiden.

De vierde paragraaf, eerste lid, bepaalt dat de leidinggevende officier van gerechtelijke politie proces-verbaal opstelt van de uitvoering van de maatregel.

Er wordt voorzien dat alle contacten met de betrokkenen geregistreerd zullen worden. Hierdoor beschikken de opsporingsdiensten en de betrokken partijen over objectief bewijsmateriaal van de toegepaste maatregel. Zoals hierboven reeds vermeld, is deze garantie van transparantie *a posteriori* een essentieel element van deze nieuwe maatregel.

De officier van gerechtelijke politie zal de geregistreerde contacten die hij relevant acht, onder het toezicht van de procureur des Konings, overschrijven of overnemen in zijn proces-verbaal.

In het oorspronkelijke voorontwerp was de mogelijkheid ingeschreven voor de verdediging en de burgerlijke partij, zoals deze ook bestaat in het kader van de tapwetgeving (art. 90*septies*), om de geregistreerde contacten te kunnen raadplegen en om de overschrijving of weergave van bijkomende delen in een proces-verbaal te vragen. Het werd aan de procureur des Konings of de rechter gelaten om te beslissen of dit verzoek al dan niet ingewilligd kon worden. Er werden limitatieve weigeringsgronden voorzien.

Aangezien echter alle contacten van een internetinfiltratie geregistreerd worden én in het open strafdossier gevoegd worden of ter griffie neergelegd worden, is de regering van mening dat het gemeenrecht moet gelden. Zo kunnen, overeenkomstig de artikelen 21*bis* Sv. voor wat betreft het opsporingsonderzoek en 61*ter* Sv. voor wat betreft het gerechtelijk onderzoek, rechtstreeks belanghebbenden de procureur des Konings of de onderzoeksrechter verzoeken om inzage te krijgen in het dossier of er een afschrift van te ontvangen. Aan de procureur des Konings kan daarnaast steeds een willig verzoek gericht worden tot overschrijving of weergave van bijkomende delen van de geregistreerde contacten in een proces-verbaal. Diezelfde vraag kan ook aan de onderzoeksrechter gericht worden op grond van artikel 61*quinquies* Sv.

De vijfde paragraaf betreft het geval waarin de maatregel wordt bevolen door de onderzoeksrechter. Net zoals dit principe van toepassing is bij de bijzondere opsporingsmethoden observatie en infiltratie, wordt de machtiging van de onderzoeksrechter ten uitvoer gelegd door de procureur des Konings, die tevens – in

dossier confidentiel, qui mentionnent également cette phrase. L'omission de cette phrase pourrait mener à un raisonnement *a contrario*.

Le quatrième paragraphe, alinéa 1er, dispose que l'officier de police judiciaire dirigeant rédige le procès-verbal de l'exécution de la mesure.

Il est prévu que tous les contacts avec les intéressés seront enregistrés. De ce fait, les services de recherche et les parties concernées disposent d'éléments de preuve objectifs concernant la mesure appliquée. Comme indiqué plus haut, cette garantie de transparence *a posteriori* est un élément essentiel de cette nouvelle mesure.

L'officier de police judiciaire retranscrira ou reproduira dans son procès-verbal les contacts enregistrés qu'il juge pertinents, sous la surveillance du procureur du Roi.

Dans l'avant-projet initial figurait la possibilité pour la défense et la partie civile, comme elle existe déjà dans le cadre de la législation sur les écoutes téléphoniques (art. 90*septies*), de pouvoir consulter les contacts enregistrés et demander la copie ou reproduction de parties supplémentaires d'un procès-verbal. La décision d'admettre ou non cette requête avait été laissée au procureur du Roi ou au juge. Des causes limitatives de rejet avaient été prévues.

Toutefois, étant donné que tous les contacts d'une infiltration via Internet sont enregistrés et sont joints au dossier pénal ouvert ou déposés au greffe, le gouvernement est d'avis que le doit commun doit s'appliquer. Ainsi, conformément aux articles 21*bis*, CIC, pour ce qui concerne l'information et 61*ter*, CIC, pour ce qui concerne l'instruction, des personnes directement intéressées peuvent demander au procureur du Roi ou au juge de consulter le dossier ou d'en obtenir une copie. En outre, il est toujours possible d'adresser une demande au procureur du Roi afin d'obtenir copie ou reproduction de parties supplémentaires des contacts enregistrés dans un procès-verbal. La même demande peut être adressée au juge d'instruction sur la base de l'article 61*quinquies*, CIC.

Le cinquième paragraphe concerne le cas où la mesure est ordonnée par le juge d'instruction. De la même manière que ce principe est applicable dans le cadre des méthodes particulières de recherche d'observation et d'infiltration, l'autorisation du juge d'instruction est mise à exécution par le procureur du Roi, qui – le cas échéant

voorkomend geval – ten aanzien van de betrokken politieambtenaren een machtiging verleent tot het plegen van strafbare feiten.

Artikel 8

Drie kleine wijzigingen worden aangebracht in artikel 47*sexies*, § 3 van het Wetboek van strafvordering, betreffende de observatie..

Ten eerste: wijziging i.v.m. proactief onderzoek

Paragraaf 3 somt een aantal vermeldingen op die de machtiging tot observatie moet bevatten.

De eerste vermelding betreft "*de ernstige aanwijzingen van het strafbaar feit die de observatie wettigen*". Uit de machtiging moet bijvoorbeeld blijken dat, indien men wil observeren met gebruik van technische hulpmiddelen, er ernstige aanwijzingen zijn dat de strafbare feiten een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben. Dit is immers de proportionaliteit die vereist wordt door artikel 47*sexies*, § 2, tweede lid Sv.

Indien men een observatie wil uitvoeren met gebruik van technische hulpmiddelen om zicht te verwerven in een woning (in welk geval de machtiging uitgaat van de onderzoeksrechter), moet uit de machtiging blijken dat er ernstige aanwijzingen zijn dat de strafbare feiten een misdrijf uitmaken of zouden uitmaken zoals bedoeld in artikel 90*ter*, § § 2, 3 en 4 Sv. of gepleegd worden of zouden worden in het kader van een criminele organisatie, zoals omschreven in artikel 324*bis* Sw. Dit blijkt uit artikel 56*bis*, tweede lid Sv.

Artikel 47*ter*, § 1, tweede lid Sv verankert het principe dat de bijzondere opsporingsmethoden ook gebruikt kunnen worden tijdens het proactief onderzoek, zoals omschreven in artikel 28*bis*, § 2 Sv. Niettemin zal dit enkel mogelijk zijn indien aan de voorwaarden van artikel 28*bis*, § 2 Sv. voldaan is, en het dus gaat om misdrijven als bedoeld in artikel 90*ter*, § § 2, 3 en 4 Sv. of gepleegd in het kader van een criminele organisatie, ook indien men bijvoorbeeld enkel een observatie met gebruik van technische hulpmiddelen wenst aan te wenden (waarvoor in artikel 47*sexies* Sv. slechts een hoofdgevangenisstraf van één jaar of een zwaardere straf vereist is). Vandaar dat bij de parlementaire bespreking van de wet van 6 januari 2003 bij amendement werd toegevoegd dat, indien de observatie zich situeert in het proactieve onderzoek zoals omschreven in artikel 28*bis*, § 2 Sv., de machtiging eveneens "de bijzondere aanwijzingen

– accorde lui aussi une autorisation de commettre des infractions aux fonctionnaires de police concernés.

Article 8

Trois petites modifications sont apportées à l'article 47*sexies*, § 3, du Code d'instruction criminelle, concernant l'observation.

Premièrement, une modification concernant l'enquête proactive

Le paragraphe 3 énumère un certain nombre d'éléments que doit mentionner l'autorisation d'observation.

La première mention concerne les "*indices sérieux de l'infraction justifiant l'observation*". À titre d'exemple, il doit ressortir de l'autorisation que, si l'on veut procéder à une observation à l'aide de moyens techniques, il doit exister des indices sérieux que les infractions peuvent donner lieu à un emprisonnement correctionnel principal d'un an ou à une peine plus lourde. Telle est en effet la proportionnalité requise par l'article 47*sexies*, § 2, alinéa 2, du Code d'instruction criminelle.

Si l'on souhaite procéder à une observation à l'aide de moyens techniques afin d'avoir une vue dans un domicile (auquel cas l'autorisation émane du juge d'instruction), il doit ressortir de l'autorisation qu'il existe des indices sérieux que les infractions constituent ou constitueraient une infraction visée à l'article 90*ter*, § § 2, 3 et 4, du Code d'instruction criminelle ou sont ou seraient commis dans le cadre d'une organisation criminelle définie à l'article 324*bis* du Code pénal. C'est ce qui ressort de l'article 56*bis*, alinéa 2, du Code d'instruction criminelle.

L'article 47*ter*, § 1er, alinéa 2, du Code d'instruction criminelle ancre le principe selon lequel les méthodes particulières de recherche peuvent également être utilisées durant une enquête proactive, comme défini à l'article 28*bis*, § 2, du Code d'instruction criminelle. Ce ne sera toutefois possible que si les conditions visées à l'article 28*bis*, § 2, précité sont réunies et que, par conséquent, il s'agit d'infractions visées à l'article 90*ter*, § § 2, 3 et 4, du même Code ou commises dans le cadre d'une organisation criminelle, y compris si on souhaite, par exemple, uniquement avoir recours à une observation à l'aide de moyens techniques (infractions pour lesquelles l'article 47*sexies* du Code d'instruction criminelle prévoit seulement un emprisonnement principal d'un an ou une peine plus lourde). D'où le fait que lors de l'examen au Parlement de la loi du 6 janvier 2003, il a été ajouté par voie d'amendement que si l'observation s'inscrit dans

met betrekking tot de elementen omschreven in deze laatste bepaling" dient te bevatten. Deze "bijzondere aanwijzingen" hebben dus betrekking op het specifieke toepassingsgebied van de proactieve recherche.

Niettemin stelt er zich nog een ander probleem bij het opstellen van de machtiging wanneer de observatie zich situeert in de proactieve recherche. Immers, wanneer de procureur des Konings een observatie wenst te machtigen in de fase van de proactieve recherche, vereist artikel 28bis, § 2 Sv. enkel een "redelijk vermoeden van te plegen of reeds gepleegde maar nog niet aan het licht gebrachte strafbare feiten". Dit stelde de magistraten voor een probleem bij het opstellen van de machtiging, aangezien de wet vereist dat de machtiging "ernstige aanwijzingen" dient te vermelden. De voorgestelde wijziging beoogt deze onduidelijkheid hierover weg te werken.

Samengevat: wanneer een magistraat een machtiging tot observatie in een proactief onderzoek opstelt, dient de machtiging voortaan het volgende te vermelden:

— het redelijke vermoeden van te plegen of reeds gepleegde maar nog niet aan het licht gebrachte strafbare feiten, en

— de bijzondere aanwijzingen met betrekking tot de elementen omschreven in artikel 28*bis*, § 2 Sv. m.a.w. de verwijzing naar het toepassingsgebied van de proactieve recherche.

De machtiging tot observatie in een reactief onderzoek dient enkel de ernstige aanwijzingen te vermelden die de observatie wettigen.

Ten tweede: periode van observatie

De tweede wijziging betreft de periode waarin de observatie kan worden uitgevoerd, en die in de huidige stand van zaken niet langer mag zijn dan één maand te rekenen van de datum van de machtiging (artikel 47*sexies*, § 3, 5° Sv.).

Aangezien de infiltratie, die in de meeste gevallen gepaard gaat met een observatie, gemachtigd kan worden voor een periode van drie maanden, acht de regering het wenselijk om ook de duur van de observatie tot drie maand te verlengen. Zoals nu al het geval is, staat het de magistraat altijd vrij om deze periode in te korten als blijkt dat de observatie van kortere duur zal zijn dan aangegeven in zijn machtiging.

le cadre de l'enquête proactive définie à l'article 28*bis*, § 2, du Code d'instruction criminelle, l'autorisation doit également contenir "*les indices particuliers relatifs aux éléments décrits dans cette dernière disposition*". Ces "indices particuliers" concernent donc le champ d'application spécifique de l'enquête proactive.

Néanmoins, un autre problème se pose encore au niveau de la rédaction de l'autorisation lorsque l'observation s'inscrit dans le cadre de l'enquête proactive. En effet, lorsque le procureur du Roi souhaite autoriser une observation au stade de l'enquête proactive, l'article 28*bis*, § 2, requiert seulement une "suspicion raisonnable que des faits punissables vont être commis ou ont été commis mais ne sont pas encore connus". Cela posait au magistrat un problème lors de la rédaction de l'autorisation vu que la loi requiert que soient mentionnés des "indices sérieux". La modification proposée vise à supprimer ce manque de clarté en la matière.

En résumé: lorsqu'un magistrat rédige une autorisation d'observation dans le cadre d'une enquête proactive, l'autorisation doit désormais mentionner ce qui suit:

— la suspicion raisonnable que des faits punissables vont être commis ou ont été commis mais ne sont pas encore connus, et

— les indices particuliers relatifs aux éléments décrits à l'article 28*bis*, § 2, du Code d'instruction criminelle, autrement dit, le renvoi au champ d'application de l'enquête proactive.

L'autorisation d'observation dans le cadre d'une enquête réactive doit uniquement mentionner les indices sérieux qui justifient l'observation.

Deuxièmement, la période d'observation

La deuxième modification porte sur la période au cours de laquelle l'observation peut être effectuée et qui, dans la situation actuelle, ne peut excéder un mois à compter de la date de l'autorisation (article 47*sexies*, § 3, 5°, du Code d'instruction criminelle).

Vu que l'infiltration, qui dans la plupart des cas s'accompagne d'une observation, peut être autorisée pour une période de trois mois, le gouvernement estime souhaitable de porter également la durée de l'observation à trois mois. Comme c'est déjà le cas à l'heure actuelle, le magistrat est toujours libre d'écourter cette période s'il s'avère que l'observation durera moins longtemps que ce qui est indiqué dans son autorisation.

De wijziging beoogt verder de administratieve werklast van de magistraat en de politie te verminderen.

Er werd immers in de praktijk vastgesteld dat in 65 % van de gevallen inzake observatie, bijna twee derden dus, een machtiging tot verlenging van de observatie wordt aangevraagd en opgemaakt moet worden. In dossiers van georganiseerde criminalilteit is een degelijke beeldvorming een noodzakelijk maar tijdrovend onderdeel van de dossieropbouw, en blijkt het onmogelijk om dit binnen één maand te verwezenlijken. Indien het een observatie met technische hulpmiddelen betreft, wat enige voorbereiding vergt, is het materiaal bovendien vaak pas of zelfs nog niet geïnstalleerd na het verlopen van de eerste machtiging.

De administratieve werklast die gepaard gaat met een verlenging is aanzienlijk. Op politioneel niveau moet er nu elke maand een vertrouwelijk verslag opgesteld worden met de vraag de machtiging te verlengen. Daarnaast moet een proces-verbaal opgemaakt worden dat het bestaan van de machtiging bevat, alsook elke wijziging, intrekking, verlenging en aanvulling. Op niveau van het parket en de onderzoeksrechter moet elke maand een nieuwe machtiging inzake observatie worden opgesteld. Ingeval de machtiging uitgaat van de onderzoeksrechter, moet het parket deze telkens ten uitvoer leggen. Tevens moet er een beslissing opgesteld worden betreffende de strafbare feiten die de politiediensten mogen plegen. Tenslotte moet een beslissing opgemaakt worden ten behoeve van het open strafdossier, die het bestaan van de machtiging bevestigt.

De verlenging van de termijn van observatie van één naar drie maanden levert dus een merkbare tijdswinst op voor de opsporingsdiensten, waardoor kostbare capaciteit vrijkomt voor andere taken en dossiers.

Tot slot wordt een technische correctie aangebracht in § 5. Er wordt immers foutief verwezen naar “het eerste lid”; In het oorspronkelijke ontwerp van wet was § 5 een lid bij § 3. Tijdens het parlementaire debat zijn bepaalde “leden” paragrafen geworden. Er moet dus verwezen worden naar § 3.

Artikel 9

De infiltratie kan nu al gebruikt worden tijdens de proactieve recherche. Dit principe is verankerd in artikel 47*ter*, § 2 Sv.

Dit artikel wijzigt artikel 47*octies*, § 3, 1° Sv. in dezelfde zin als artikel 47*sexies*, § 3, 1° Sv. gewijzigd werd door artikel 8.

La modification vise en outre à réduire la charge de travail administrative du magistrat et de la police.

Il a en effet été constaté dans la pratique que dans 65 % des observations, soit près de 2/3 des cas donc, une autorisation de prolongation de l’observation est demandée et doit être rédigée. Dans des dossiers de criminalinté organisée, une bonne vision de la situation est un élément nécessaire pour constituer le dossier mais qui prend énormément de temps, ce qui s’avère irréalisable en un seul mois. En outre, dans le cas d’une observation effectuée à l’aide de moyens techniques, qui exige une certaine préparation, le matériel est souvent à peine installé, voire pas encore, lorsque la première autorisation expire.

La charge de travail administrative associée à une prolongation est considérable. Au niveau de la police, un rapport confidentiel doit à présent être rédigé tous les mois avec la demande d’autorisation de prolongation. En outre, un procès-verbal doit être dressé dans lequel figurent l’existence de l’autorisation ainsi que toute modification, tout retrait, toute prolongation et tout ajout. Au niveau du parquet et du juge d’instruction, une nouvelle autorisation d’observation doit être rédigée tous les mois. Si l’autorisation émane du juge d’instruction, le parquet doit chaque fois l’exécuter. Une décision concernant les infractions que les services de police peuvent commettre doit également être rédigée. Enfin, une décision confirmant l’existence de l’autorisation doit être rédigée pour le dossier répressif ouvert.

La prolongation du délai de l’observation d’un à trois mois apporte donc un gain de temps notable pour les services de recherche, libérant ainsi une précieuse capacité pour d’autres tâches et dossiers.

Enfin, une correction technique est apportée au § 5. En effet, on y réfère erronément à “l’alinéa 1er”. Dans le texte initial du projet, le § 5 était un alinéa du § 3. Lors des discussions parlementaires, certains “alinéas” sont devenus des paragraphes. Il faut donc faire référence au § 3.

Article 9

L’infiltration peut déjà être utilisée pendant l’enquête proactive. Ce principe est ancré à l’article 47*ter*, § 2, du Code d’instruction criminelle.

Cet article modifie l’article 47*octies*, § 3, 1°, du Code d’instruction criminelle dans le même sens que la modification de l’article 47*sexies*, § 3, 1°, par l’article 8.

Wanneer een magistraat een machtiging tot infiltratie in een proactief onderzoek opstelt, moet de machtiging voortaan het redelijk vermoeden vermelden van te plegen of reeds gepleegde maar nog niet aan het licht gebrachte strafbare feiten, alsook de bijzondere aanwijzingen met betrekking tot de elementen omschreven in artikel 28*bis*, § 2 Sv. die de infiltratie wettigen. Er kan ook verwezen worden naar de uitleg onder artikel 8.

In § 5 wordt dezelfde technische correctie aangebracht als in artikel 47*septies*.

Artikel 10

Artikel 47*undecies*, laatste lid, Sv voorziet in een controle door het College van procureurs-generaal over alle dossiers waarin de informantenwerking in overeenstemming met artikel 47*decies*, § 7 Sv. werd toegepast. Dit zijn dossiers waarbij het plegen van misdrijven door informanten werd gemachtigd. Aangezien de laatstgenoemde bepaling vernietigd werd door het Grondwettelijk Hof (arrest nr. 105/2007 van 19 juli 2007), heeft deze controle geen bestaansreden meer. Artikel 47*undecies*, laatste lid Sv. dient dan ook te worden opgeheven.

Noot: bij hetzelfde arrest van het Grondwettelijk Hof waren de tweede zin van lid twee en van lid drie van art. 47*undecies* Sv. reeds uitdrukkelijk geschrapt. Die bepalingen handelden over de toepassing van de bijzondere opsporingsmethoden in het kader van de strafuitvoering.

Artikel 11

Net zoals het geval is voor de bijzondere opsporingsmethoden, wordt voor de infiltratie op internet (artikel 46*sexies* Sv.) voorzien in een uitzondering op artikel 56, § 1, derde lid Sv. en kunnen de machtigingen van de onderzoeksrechter in dit kader ten uitvoer worden gelegd door de procureur de Konings.

Ook wordt een geheimhoudingsplicht ingeschreven voor de stafhouder en de vertegenwoordiger van de provinciale orde van geneesheren, wanneer zij op de hoogte worden gebracht van een maatregel zoals bedoeld in artikel 56*bis*, derde lid Sv.

Volgens de Raad van State lijken deze personen reeds onder het toepassingsgebied van artikel 458 te vallen. Niettemin lijkt het de regering aangewezen om dit expliciet te verduidelijken, naar analogie met de geheimhoudingsplicht van andere personen die meewerken

Si un magistrat rédige une autorisation d'infiltration dans le cadre d'une enquête proactive, l'autorisation doit dorénavant mentionner la suspicion raisonnable que des faits punissables vont être commis ou ont été commis mais ne sont pas encore connus ainsi que les indices particuliers relatifs aux éléments décrits à l'article 28*bis*, § 2, du Code d'instruction criminelle qui justifient l'infiltration. Il peut dès lors être renvoyé au commentaire de l'article 8.

Au § 5, la même correction technique est apportée qu'à l'article 47*septies*.

Article 10

L'article 47*undecies*, dernier alinéa, du Code d'instruction criminelle prévoit un contrôle du Collège des procureurs généraux sur tous les dossiers dans lesquels le recours aux indicateurs conformément à l'article 47*decies*, § 7, du même Code a été mis en œuvre. Il s'agit de dossier autorisant la commission d'infractions par des indicateurs. Cette dernière disposition ayant été annulée par la Cour constitutionnelle (arrêt n° 105/2007 du 19 juillet 2007), ce contrôle n'a plus de raison d'être. L'article 47*undecies*, dernier alinéa, du Code d'instruction criminelle doit dès lors être abrogé.

Note: le même arrêt de la Cour constitutionnelle abrogeait déjà explicitement la deuxième phrase de l'alinéa 2 et de l'alinéa 3 de l'article 47*undecies* du Code d'instruction criminelle. Ces dispositions traitaient de l'application des méthodes particulières de recherche dans le cadre de l'exécution des peines.

Article 11

Tout comme c'est le cas pour les méthodes particulières de recherche, il est prévu pour l'infiltration sur Internet (article 46*sexies* du Code d'instruction criminelle) une exception à l'article 56, § 1er, alinéa 3, dudit Code et les autorisations du juge d'instruction dans ce cadre peuvent être exécutées par le procureur du Roi.

Il est également prévu une obligation de secret pour le bâtonnier et le représentant de l'ordre provincial des médecins lorsqu'ils sont avertis d'une mesure visée à l'article 56*bis*, alinéa 3, du Code d'instruction criminelle.

Selon le Conseil d'État, ces personnes semblent déjà relever du champ d'application de l'article 458. Néanmoins, il paraît indiqué au gouvernement de le préciser de manière explicite, par analogie avec le respect du secret auquel sont tenus d'autres personnes

met de gerechtelijke autoriteiten (zoals bijvoorbeeld operatoren van elektronische communicatienetwerken).

Artikel 12

Artikel 88*bis* wordt in dezelfde zin gewijzigd als artikel 46*bis* (zie de uitgebreide toelichting bij dit artikel). De term "verstrekker van een elektronische communicatiedienst" wordt vervangen door een nieuwe, ruimere omschrijving die overeenstemt met de interpretatie van het Hof van Cassatie in zijn "Yahoo-arrest" van 18/01/2011. Daarnaast wordt de termijn voor het verlenen van medewerking aangepast naar "in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering".

Ook wordt een geheimhoudingsplicht ingeschreven voor de stafhouder en de vertegenwoordiger van de provinciale orde van geneesheren, wanneer zij op de hoogte worden gebracht van een maatregel.

In artikel 88*bis*, § 1, zesde lid, wordt artikel 434 toegevoegd aan de misdrijven waarvoor de procureur des Konings de maatregel zelf kan bevelen in geval van ontdekking op heterdaad. Deze artikelen worden ook toegevoegd in artikel 90*ter*, § 5 van het Wetboek van strafvordering.

Tot slot wordt in het laatste lid van § 1 een technische correctie uitgevoerd.

Voor de wijziging in § 4, eerste lid, betreffende de termijn waarbinnen de gegevens meegedeeld worden, kan verwezen worden naar de uitleg bij artikel 46*bis*.

Artikel 13

Artikel 88*ter* van het Wetboek van strafvordering wordt bij dit artikel opgeheven, aangezien het geïntegreerd werd in artikel 39*bis*.

Artikel 14

Door de wijzigingen aan artikel 39*bis* Sv, moet ook artikel 88*quater* Sv. worden aangepast, met betrekking tot de uitbreiding van de zoeking in een informaticasysteem of een deel ervan.

De maximum gevangenisstraf voorzien in het eerste lid van § 3 voor de niet-medewerking of het verhinderen

qui collaborent avec les autorités judiciaires (comme par exemple les opérateurs de réseaux de communications électroniques).

Article 12

L'article 88*bis* est modifié dans le même sens comme l'article 46*bis* (voir commentaire détaillé de cet article). Les termes "fournisseur d'un service de communications électroniques" sont remplacés par une nouvelle définition, plus large, conforme à l'interprétation de la Cour de cassation dans son "arrêt Yahoo" du 18/01/2011. En outre, le délai pour prêter sa collaboration est adapté et devient "en temps réel ou, le cas échéant, au moment précisé dans la réquisition".

Il est également prévu une obligation de secret pour le bâtonnier et le représentant de l'ordre provincial des médecins lorsqu'ils sont avertis d'une mesure.

A l'article 88*bis*, § 1er, alinéa 6, l'article 434 est ajouté aux infractions pour lesquelles le procureur du Roi peut ordonner lui-même la mesure en cas de prise en flagrant délit. Ces articles sont également ajoutés à l'article 90*ter*, § 5, du Code d'instruction criminelle.

Enfin, une correction technique est apportée au dernier alinéa du § 1er.

Pour la référence au § 4, alinéa 1er, relatif au délai dans lequel les données sont communiquées, on peut renvoyer à l'explication donnée pour l'article 46*bis*.

Article 13

L'article 88*ter* du code d'instruction criminelle est abrogé par cet article étant donné qu'il a été intégré dans l'article 39*bis*.

Article 14

Les modifications apportées à l'article 39*bis* du Code d'instruction criminelle imposent également l'adaptation de l'article 88*quater* du même Code en ce qui concerne l'extension de la recherche dans un système informatique ou une partie de celui-ci.

L'emprisonnement maximum prévu à l'alinéa 1er du § 3 pour refus de collaboration ou entrave à la recherche

van de zoeking in het informaticasysteem of de uitbreiding ervan, wordt opgetrokken van één jaar tot drie jaar.

Tevens wordt door het voorontwerp van wet een nieuw, tweede lid toegevoegd aan § 3 waarin een gevangenisstraf wordt bepaald van één tot vijf jaar en een geldboete van vijfhonderd tot vijftigduizend euro wanneer de niet-medewerking of het verhinderen van de zoeking in het informaticasysteem of de uitbreiding ervan, de uitvoering van een misdaad of wanbedrijf kan verhinderen, of de gevolgen ervan kan beperken.

Deze strengere bestraffing moet een duidelijk signaal geven aan personen die hun medewerking niet verlenen of die het onderzoek dwarsbomen.

In veel gevallen is de gevorderde medewerking immers van groot belang voor het onderzoek. Gelet op de huidige stand van de technologie en de verdere evolutie die op dit domein nog mag worden verwacht, is het voor de opsporingsdiensten vaak bijzonder moeilijk of zelfs onmogelijk om toegang te verkrijgen tot gegevens op een informaticasysteem, zonder hulp van externen die op de hoogte zijn van de werking ervan, de gebruikte versleuteling etc.

In punt 34 van zijn advies vraagt de Raad van State meer toelichting omtrent het toepassingsgebied van artikel 88*ter*, naar aanleiding van de vervanging van het woord “personen” door de woorden “aan eenieder”.

Het voorontwerp spreekt over “eenieder”, dus ook rechtspersonen worden beoogd. Voor het overige wijzigt het voorontwerp niets aan het toepassingsgebied van dit artikel zoals verduidelijkt in de memorie van toelichting bij de wet inzake informaticacriminaliteit: “In antwoord op de Raad van State moet gesteld worden dat de kring van personen die geviseerd worden door artikel 88*quater* niet in abstracto kan worden omschreven: het kan gaan om importeurs/verdelers van computers of software, ‘trusted third parties”, dienstenverstrekkers, operatoren, bedrijfsingenieurs die een specifieke informaticaconfiguratie hebben uitgewerkt, beveiligingsspecialisten, …

De onderzoeksrechter zal dit geval per geval moeten nagaan. Bovendien gaat het uiteraard slechts om een inspanningsverbintenis: men kan immers niet meer van iemand verlangen dan hij zelf vermag’ (*Parl St.* Kamer 1992-2000, 50-213/001, p. 27).

Hetzelfde geldt overigens voor artikel 90*ter*, § 4.

dans le système informatique ou à son extension est porté d’un an à trois ans.

L’avant-projet de loi complète également le § 3 par un alinéa 2 qui prévoit un emprisonnement d’un an à cinq ans et une amende de cinq cents euros à cinquante mille euros si le refus de collaboration ou l’entrave à la recherche dans un système informatique ou à son extension peut empêcher la commission d’un crime ou d’un délit ou en limiter les effets.

Cette sanction plus sévère doit envoyer un signal clair aux personnes qui ne prêtent pas leur collaboration ou qui sapent l’enquête.

Dans de nombreux cas, la collaboration requise est en effet essentielle pour l’enquête. Compte tenu de l’état actuel de la technologie et de son évolution attendue dans ce domaine, il est souvent particulièrement difficile pour les services de recherche, voire impossible, d’accéder à des données d’un système informatique sans l’aide d’externes qui en connaissent le fonctionnement, qui savent quel est le cryptage utilisé, etc.

Au point 34 de son avis, le Conseil d’État demande de donner plus de précisions concernant le champ d’application de l’article 88*ter*, suite au remplacement des mots “aux personnes” par les mots “à quiconque”.

Comme l’avant-projet parle de “quiconque”, les personnes morales sont également visées. Pour le surplus, l’avant-projet ne modifie en rien le champ d’application de cet article, comme on l’explique dans l’exposé des motifs de la loi relative à la criminalité informatique: “En réponse à l’avis du Conseil d’État, il y a lieu de préciser que le cercle de personnes visées par l’article 88*quater* ne peut être décrit in abstracto: il peut s’agir d’importateurs/de distributeurs d’ordinateurs ou de logiciels, de “trusted third parties”, de fournisseurs de service, d’opérateurs, d’ingénieurs d’entreprise ayant élaboré une configuration informatique spécifique, de spécialistes de la sécurité, …

Le juge d’instruction devra faire les vérifications au cas par cas. De plus, il ne s’agit, bien évidemment, que d’un engagement à fournir des efforts: on ne peut attendre d’une personne qu’elle fournisse des efforts qu’elle est incapable de fournir.” (*Doc. parl.*, Chambre 1992-2000, 50-213/001, p. 27).

Il en va de même pour l’article 90*ter*, § 4.

Artikel 15

Naar analogie met artikel 46*quinquies* van het Wetboek van strafvordering wordt ook artikel 89*ter* van hetzelfde wetboek, dat betrekking heeft op de andere private plaatsen dan die bedoeld in artikel 46*quinquies*, § 1 Sv. en bijgevolg enkel tot de bevoegdheid van de onderzoeksrechter behoort, uitgebreid tot het openen van gesloten voorwerpen die zich op deze plaats bevinden.

Artikel 46*quinquies* Sv werd ingevoerd met de BOM-reparatiewet van 27 december 2005, en er werd aldus een onderscheid gemaakt tussen enerzijds de private plaats die geen woning of aanhorigheid ervan is en, anderzijds, de private plaats die dit wel is. De private plaats in de zin van artikel 46*quinquies* Sv. wordt gedefinieerd in het artikel zelf (artikel 46*quinquies*, § 1, tweede lid). Huidig voorontwerp brengt op dit vlak geen wijzigingen aan in de reeds bestaande wetgeving.

Tevens wordt er door het wetsontwerp een nieuwe mogelijkheid gecreëerd tot een heimelijke “zoeking” in een informaticasysteem, evenwel enkel met het oog op de doeleinden vermeld in artikel 46*quinquies*, § 2 Sv.

De finaliteit van deze maatregel, zoals gesteld in § 2, 1° en 2° van art. 46*quinquies* Sv., is te kijken of er bewijsmateriaal bestaat, maar niet het te verzamelen. Er mogen enkel stalen genomen worden.

In het kader van een inkijkoperatie in een informaticasysteem betekent dit dat een gerichte kopie mag genomen worden van bepaalde gegevens.

Als we het voorbeeld nemen van een vaste of draagbare computer, laat de maatregel bedoeld in artikel 89*ter* bijvoorbeeld niet toe dat een kopie genomen wordt van de gehele harde schijf.

Een voorbeeld van een inkijkoperatie in een informaticasysteem in de zin van artikel 89*ter* Sv.: bij een onderzoek naar kinderpornografie of naar een pedofielennetwerk, kan het nuttig zijn dat in de computer gekeken wordt om zich ervan te vergewissen of er wel degelijk kinderpornografisch materiaal is aan te treffen of niet, om het onderzoek nadien verder te kunnen oriënteren. Staalname (kopiename) van enkele beelden kan nuttig zijn om bv. te onderzoeken of het wel degelijk gaat om kinderporno.

Het onderscheid tussen de heimelijke zoeking in een informaticasysteem zoals ingevoerd in artikel 89*ter* Sv.

Article 15

Par analogie avec l’article 46*quinquies* du Code d’instruction criminelle, l’article 89*ter* du même Code, qui a trait aux lieux privés autres que ceux visés à l’article 46*quinquies*, § 1er, et qui relèvent donc de la compétence exclusive du juge d’instruction, est également étendu à l’ouverture du contenu d’objets fermés se trouvant sur place.

L’article 46*quinquies* du Code d’instruction criminelle a été introduit avec la loi de réparation MPR du 27 décembre 2005 et une distinction a ainsi été établie entre, d’une part, le lieu privé qui n’est pas un domicile ou une dépendance de domicile et, d’autre part, le lieu privé qui est un domicile ou une dépendance de ce domicile. Le lieu privé au sens de l’article 46*quinquies* du Code d’instruction criminelle est défini dans l’article même (article 46*quinquies*, § 1er, alinéa 2). Le présent projet n’apporte pas de modification sur ce plan à la législation existante.

Le projet de loi instaure également une nouvelle possibilité de “recherche” en secret dans un système informatique, mais uniquement aux fins mentionnées à l’article 46*quinquies*, § 2, du Code d’instruction criminelle.

La finalité de cette mesure, précisée au § 2, 1° et 2°, de l’article 46*quinquies* du Code d’instruction criminelle, est de voir si des preuves existent mais pas de les collecter. Seuls des échantillons peuvent être prélevés.

Dans le cadre d’un contrôle visuel discret dans un système informatique, cela signifie qu’il peut être pris une copie ciblée de certaines données.

Si on prend l’exemple d’un ordinateur fixe ou portable, la mesure visée à l’article 89*ter* ne permet par exemple pas de prendre une copie complète de tout le disque dur.

On peut citer comme exemple de contrôle discret dans un système informatique au sens de l’article 89*ter* du Code d’instruction criminelle la situation suivante: dans le cadre d’une recherche de pédopornographie ou de la recherche d’un réseau de pédophiles, il peut être utile de regarder dans l’ordinateur pour vérifier si on y trouve du matériel pédopornographique ou non, afin de pouvoir ensuite orienter l’enquête. Le prélèvement (prise de copie) de quelques images peut s’avérer utile pour examiner par exemple s’il s’agit bien de pornographie enfantine.

La distinction entre la recherche en secret dans un système informatique conformément à l’article 89*ter* du

en de heimelijke zoeking in een informaticasysteem zoals ingevoerd door artikel 90*ter* Sv., ligt voornamelijk in de finaliteit van de maatregel. De finaliteit van artikel 89*ter* Sv. is dat er kan gezocht worden naar bewijs van strafbare feiten, maar het gevonden bewijs niet mag verzameld en gebruikt worden; er mogen enkel stalen worden genomen.

De inkijkoperatie in een informaticasysteem is met andere woorden een oriënterend instrument dat het mogelijk maakt om gradueel op de privacy in te breken en stalen te nemen die in voorkomend geval een nog verdergaande maatregel kunnen verantwoorden.

Er is voor geopteerd om de inkijkoperatie in een informaticasysteem onder te brengen in artikel 89*ter* en niet artikel 46*quinquies*, ook al zou in principe kunnen worden verdedigd dat een informaticasysteem – bijvoorbeeld een Hotmailaccount, een Facebook-account, een iCloud-account, … – private plaatsen zijn die géén woning zijn. Gelet op het feit dat de privacy van personen online of in de *"cloud"* dermate omvangrijk en gevoelig kan zijn, gecombineerd met het feit dat deze privacy bij een inkijkoperatie "heimelijk" wordt benaderd, dient dit consequent onder de controle van de onderzoeksrechter te worden gesteld.

Artikel 17

De volgende artikelen introduceren een nieuwe onderzoeksmaatregel in het Wetboek van Strafvordering, namelijk de heimelijke zoeking in een informaticasysteem.

Meer en meer wordt namelijk vastgesteld dat criminelen gebruik maken van alle mogelijkheden die de informatietechnologie hen biedt. Politiediensten en magistratuur moeten daarom over de geschikte middelen kunnen beschikken. Het voorontwerp van wet wil hier dan ook een meer aangepast juridisch kader ontwerpen voor de zoeking in een informaticasysteem, die heimelijk moet kunnen gebeuren.

Al in het arrest nr. 202/2004 van het Arbitragehof van 21 december 2004, met betrekking tot de wet van 6 januari 2003 betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden, was het Hof van oordeel dat de inkijkoperatie (artikel 89*ter* Sv.) en de observatie met gebruik van technische hulpmiddelen om zicht te verwerven in een woning (artikel 56*bis*, tweede lid Sv.) maatregelen zijn die, wat betreft de inmenging in het recht op eerbiediging van het privéleven, vergeleken kunnen worden met de huiszoeking en met het afluisteren en opnemen van privécommunicatie en -telecommunicatie. Deze maatregelen kunnen volgens

Code d'instruction criminelle et la recherche en secret dans un système informatique conformément à l'article 90*ter* du même Code réside principalement dans la finalité de la mesure. La finalité de l'article 89*ter* du Code d'instruction criminelle est de permettre la recherche de preuves d'infractions, mais les preuves découvertes ne peuvent pas être collectées, ni utilisées, et seuls des échantillons peuvent être prélevés.

En d'autres termes, le contrôle visuel discret dans un système informatique est un instrument orienté qui permet une intrusion graduelle dans la vie privée et la prise de prélèvements qui, le cas échéant, peuvent justifier une mesure encore plus intrusive.

Il a été décidé de classer le contrôle visuel discret dans un système informatique sous l'article 89*ter* et non sous l'article 46*quinquies*, bien que l'on puisse en principe défendre le fait qu'un système informatique – par exemple un compte Hotmail, un compte Facebook, un compte iCloud... – est un lieu privé qui n'est pas un domicile. Vu l'étendue et le caractère sensible de la vie privée de personnes en ligne ou dans le *"cloud"*, combinés au fait que cette vie privée peut faire l'objet d'une approche "en secret" lors d'un contrôle visuel discret, cette opération doit s'effectuer de manière cohérente sous le contrôle du juge d'instruction.

Article 17

Les articles suivants introduisent une nouvelle mesure d'enquête dans le Code d'instruction criminelle, la recherche en secret dans un système informatique.

En effet, il est de plus en plus souvent constaté que les criminels recourent à toutes les possibilités que leur offre la technologie de l'information. Les services de police et la magistrature doivent par conséquent pouvoir disposer des moyens adaptés. Le présent avant-projet de loi entend dès lors créer ici un cadre juridique plus adapté pour la recherche dans un système informatique, laquelle doit pouvoir intervenir en secret.

Déjà dans l'arrêt n° 202/2004 du 21 décembre 2004 de la Cour d'Arbitrage relatif à la loi du 6 janvier 2003 concernant les méthodes particulières de recherche et quelques autres méthodes d'enquête, la Cour a estimé que le contrôle visuel discret (article 89*ter* du Code d'instruction criminelle) et l'observation effectuée à l'aide de moyens techniques afin d'avoir une vue dans un domicile (article 56*bis*, alinéa 2, du Code d'instruction criminelle) sont des mesures qui peuvent être comparées, en ce qui concerne l'ingérence dans les droits garantissant la vie privée, à la perquisition et aux écoutes et enregistrements des communications

het Hof dan ook enkel worden toegelaten onder dezelfde voorwaarden als diegene die gelden in verband met de huiszoeking en het afluisteren van telefoongesprekken. Om die reden moeten de inkijkoperatie en de observatie met gebruik van technische hulpmiddelen om zicht te verwerven in een woning worden uitgesloten van de toepassingssfeer van het mini-onderzoek, dat het voorwerp uitmaakt van artikel 28*septies* Sv.

Dezelfde uitsluiting geldt voor de onderzoeksmaatregel van de heimelijke zoeking. Om die reden wordt deze maatregel geïntegreerd in artikel 90*ter*, § 1 Sv., dat dezelfde kenmerken vertoont.

De wijziging heeft niet enkel tot gevolg dat, naast de reeds bestaande maatregel van de interceptie van communicatie, de heimelijke zoeking in een informaticasysteem wordt toegevoegd. Ze leidt er eerder toe dat de twee maatregelen verenigd worden in één maatregel, om zich aan te passen aan de technologische evoluties die het onmogelijk maken om het verschil te maken tussen, enerzijds, de heimelijke zoeking in een informaticasysteem, en anderzijds, de interceptie van communicatie.

Het eerste lid is ingrijpend herzien met het oog op deze verandering.

PARAGRAAF 1:

LID 1: Tap en heimelijke zoeking in informaticasysyteem

Het eerste lid van § 1 omschrijft de maatregel die de onderzoeksrechter kan bevelen. Deze behelst het onderscheppen, kennis nemen van, doorzoeken en opnemen van niet voor publiek toegankelijke communicatie of van gegevens van een informaticasysteem of een deel ervan, alsook de uitbreiding van een zoeking in een informaticasysteem.

Met “niet voor publiek toegankelijke communicatie” wordt bedoeld: communicatie of elektronische communicatie die zich in de privésfeer afspeelt. Het is een overkoepelend begrip dat ook de termen “privécommunicatie of -telecommunicatie” van het oude artikel 90*ter* omvat.

De term “doorzoeken” heeft betrekking op informaticasystemen en heeft dezelfde betekenis als de uitvoering van een zoeking in een informaticasysteem.

“Opnemen” slaat zowel op het opnemen van niet voor publiek toegankelijke communicatie (zoals het maken van geluidsopnames bij telefoontap of direct afluisteren)

et télécommunications privées. Selon la Cour, ces mesures ne peuvent être autorisées qu’aux mêmes conditions que celles appliquées à l’égard de la perquisition et des écoutes téléphoniques. C’est la raison pour laquelle le contrôle visuel discret et l’observation effectuée à l’aide de moyens techniques afin d’avoir une vue dans un domicile sont exclus du champ d’application de la mini-instruction, qui fait l’objet de l’article 28*septies* du Code d’instruction criminelle.

Cette exclusion s’applique à la mesure d’enquête de la recherche en secret. C’est pourquoi cette mesure est intégrée dans l’article 90*ter*, § 1er, du Code d’instruction criminelle, qui présente les mêmes caractéristiques.

La modification n’aboutit pas seulement à ajouter la recherche secrète dans un système informatique à côté de la mesure déjà existante de l’interception des communications. Elle aboutit plutôt à fusionner les deux mesures en une seule afin de s’adapter aux évolutions technologiques qui rendent impossible la distinction entre, d’une part, la recherche dans un système informatique et, d’autre part, l’interception des communications.

Le paragraphe 1er a été largement remanié en vue de ce changement.

PARAGRAPHE 1ER:

ALINÉA 1ER: Écoutes téléphoniques et recherche en secret dans un système informatique

L’alinéa 1er du paragraphe 1er décrit la mesure que le juge d’instruction peut ordonner. Celle-ci comprend l’interception, la prise de connaissance, l’exploration et l’enregistrement de communications non accessibles au public ou de données d’un système informatique ou d’une partie de celui-ci, ainsi que l’extension d’une recherche dans un système informatique.

Il convient d’entendre par “communications non accessibles au public” des communications ou communications électroniques qui ont lieu dans la sphère privée. Il s’agit d’une notion globale qui recouvre également les termes “communications ou télécommunications privées” de l’ancien article 90*ter*.

Le terme “explorer” se rapporte aux systèmes informatiques et a la même signification que l’exécution d’une recherche dans un système informatique.

Le terme “enregistrer” porte tant sur les communications non accessibles au public (comme les enregistrements sonores dans le cadre d’écoutes téléphoniques

als op het registreren of kopiëren van gegevens van een informaticasysteem (zoals het kopiëren van afbeeldingen, documenten etc. van een computer op een USB-stick). Het is dus een methode om het (bewijs)materiaal te verzamelen dat via de toepassing van de maatregel van artikel 90*ter* is verkregen.

De zinsnede "tijdens de overbrenging [van de communicatie]", die voorkomt in het bestaande artikel 90*ter*, § 1, eerste lid, werd bewust niet behouden. Door de nieuwe ontwikkelingen op informaticagebied is het immers vaak onmogelijk geworden om uit te maken wanneer communicatie nog "in overbrenging" is, dan wel reeds afgeleverd. Voorbeeld: moet een ongelezen e-mail beschouwd worden als afgeleverde communicatie of als communicatie die wordt overgebracht?

De maatregel van artikel 90*ter*, § 1, eerste lid wordt steeds bevolen met een heimelijk oogmerk. Dit betekent dat de onderzoeksrechter de *bedoeling* heeft, via intrusie en stiekeme bewaking, kennis te nemen van communicatie of gegevens buiten medeweten van de deelnemers aan die communicatie of buiten medeweten van de eigenaar, de bezitter of de gebruiker van het informaticasysteem.

In samenlezing met de zinsnede "onverminderd de toepassing van [artikel] 39*bis*" betekent dit dat niet elke zoeking in een informaticasysteem, die zou plaatsvinden buiten medeweten van de eigenaar, de bezitter of de gebruiker van dit systeem, door de onderzoeksrechter dient te worden gemachtigd conform artikel 90*ter*. Er zijn immers situaties denkbaar waarbij het heimelijk *oogmerk* afwezig is.

Voorbeeld: De politie doet een zoeking in een inbeslaggenomen wagen en vindt hierin een gsm, waarvan de eigenaar niet gekend is. Deze gsm mag doorzocht worden op grond van artikel 39*bis*, ook al is de eigenaar daarvan niet op de hoogte. De *doelstelling* is immers niet dat de maatregel heimelijk zou worden uitgevoerd. De zoeking is reactief en onmiddellijk, weliswaar in afwezigheid van de eigenaar of gebruiker. Er is geen verplichting om in die omstandigheden eerst een zoektocht te lanceren naar de houder van het informaticasysteem: het werd aangetroffen overeenkomstig de wet en is exploiteerbaar overeenkomstig de wet. Indien de eigenaar of gebruiker wordt aangetroffen, zal hem kennis worden gegeven van de onderzoekingen.

De zinsnede "onverminderd de toepassing van artikelen 87, 88, 89*bis* en 90" impliceert dat artikel 90*ter* geen afbreuk doet aan de bevoegdheden van de onderzoeksrechter inzake huiszoeking. Bij de huiszoeking kunnen dus ook, bij wijze van voorbeeld, gegevens van

ou les écoutes directes) que sur l'enregistrement ou la copie de données d'un système informatique (comme la copie d'images, de documents... d'un ordinateur sur une clé USB). Il s'agit donc d'une méthode de collecte de matériel (de preuves) obtenu(es) par l'application de la mesure de l'article 90*ter*.

Le membre de phrase "pendant leur transmission" qui figure dans l'article 90*ter*, § 1er, alinéa 1er, n'a délibérément pas été conservé. En effet, vu les dernières évolutions dans le domaine de l'informatique, il est souvent devenu impossible de déterminer quand la communication est toujours en cours de "transmission" et quand elle est déjà délivrée. Exemple: un e-mail non lu doit-il être considéré comme une communication délivrée ou comme une communication en cours de transmission?

La mesure de l'article 90*ter*, § 1er, alinéa 1er, est toujours ordonnée dans un but secret. Ceci signifie que le juge d'instruction a l'*intention* , par une intrusion et une surveillance en secret, de prendre connaissance de communications ou de données à l'insu des acteurs de ces communications ou à l'insu du propriétaire, du détenteur ou de l'utilisateur du système informatique.

Lu conjointement avec le membre de phrase "sans préjudice de l'application de l'article 39*bis*", cela signifie que toutes les recherches dans un système informatique, qui auraient lieu à l'insu du propriétaire, du détenteur ou de l'utilisateur de ce système, ne doivent pas être autorisées par le juge d'instruction conformément à l'article 90*ter*. En effet, on peut imaginer des situations où le *but* secret est absent.

Exemple: La police effectue une recherche dans une voiture saisie et y trouve un gsm dont le propriétaire n'est pas connu. Ce gsm peut être exploré sur la base de l'article 39*bis*, même si le propriétaire n'en est pas informé. L'*objectif* n'est effectivement pas que la mesure soit réalisée en secret. La recherche est réactive et immédiate, en l'absence certes du propriétaire ou de l'utilisateur. Il n'est pas obligatoire dans ces conditions d'effectuer d'abord une recherche sur le détenteur du système informatique: il a été découvert dans le respect de la loi et est exploitable conformément à celle-ci. Si l'on trouve le propriétaire ou l'utilisateur, il sera informé des recherches.

Le membre de phrase "sans préjudice de l'application des articles 87, 88, 89*bis* et 90" implique que l'article 90*ter* ne porte pas atteinte aux compétences du juge d'instruction en matière de perquisition. À titre d'exemple, les données d'un système informatique

een informaticasysteem doorzocht worden, zonder dat de toepassingsvoorwaarden van artikel 90*ter* dienen te worden nageleefd.

Er moet op gewezen worden dat het nieuwe eerste lid van art. 90*ter* zowel de zoeking in een informaticasysteem zoals bedoeld in artikel 39*bis* Sv. als de uitbreiding van een zoeking zoals bedoeld in artikel 88*ter* van hetzelfde Wetboek omvat. Wanneer de onderzoeksrechter de uitbreiding van een zoeking op een heimelijke manier beveelt, dient hij uiteraard ook na te gaan of aan de twee voorwaarden van artikel 39*bis*, § 4, eerste lid van hetzelfde Wetboek is voldaan en is de uitbreiding begrensd tot de beperkingen omschreven in artikel 39*bis*, § 4, tweede lid van hetzelfde Wetboek.

LID 2:

Het tweede lid noemt de voorwaarden waaraan moet voldaan zijn om de maatregel van artikel 90*ter*, § 1, eerste lid te kunnen bevelen.

De maatregel kan slechts worden bevolen:

— in uitzonderlijke gevallen;

— indien het onderzoek zulks vereist;

— indien er ernstige aanwijzingen bestaan dat het een feit betreft zoals opgesomd in § 2 van artikel 90 ter;

— indien de overige middelen van onderzoek niet volstaan om de waarheid aan de dag te brengen (subsidiariteit).

Dit zijn dezelfde voorwaarden die momenteel reeds gelden.

LID 3

De onderzoeksrechter kan enkele begeleidende maatregelen machtigen die de uitvoering van de maatregel van artikel 90*ter*, § 1, eerste lid mogelijk maken, en dit zowel fysiek als technisch, heimelijk, etc.

Het gaat meer bepaald om:

— het binnendringen in een woning, private plaats of informaticasysteem.

Dit laat de politiediensten bijvoorbeeld toe om zich toegang te verschaffen tot een bepaalde plaats, ook al is deze beveiligd met sloten, alarmsystemen en dergelijke meer, teneinde in die plaats afluisterapparatuur aan te brengen.

peuvent donc aussi être explorées lors de la perquisition, sans que les conditions d'application de l'article 90*ter* doivent être respectées.

Il convient de souligner que le nouvel alinéa 1er de l'article 90*ter* du Code d'instruction criminelle porte tant sur la recherche dans un système informatique visée à l'article 39*bis* que sur l'extension d'une recherche visée à l'article 88*ter* du même Code. Lorsque le juge d'instruction ordonne en secret l'extension d'une recherche, il doit bien évidemment vérifier aussi si les deux conditions de l'article 39*bis*, § 4, alinéa 1er du même Code sont remplies et si l'extension s'inscrit dans les limites définies à l'article 39*bis*, § 4, alinéa 2 du même code.

ALINÉA 2:

L'alinéa 2 cite les conditions qui doivent être remplies pour que la mesure de l'article 90*ter*, § 1er, alinéa 1er, puisse être ordonnée.

La mesure peut être ordonnée uniquement:

— à titre exceptionnel;

— lorsque les nécessités de l'instruction l'exigent;

— s'il existe des indices sérieux qu'il s'agit d'un fait visé au § 2 de l'article 90*ter*;

— si les autres moyens d'investigation ne suffisent pas à la manifestation de la vérité (subsidiarité).

Ce sont les mêmes conditions que celles en vigueur actuellement.

ALINÉA 3:

Le juge d'instruction peut autoriser quelques mesures d'accompagnement qui permettront l'exécution de la mesure de l'article 90*ter*, § 1er, alinéa 1er, ce tant physiquement que techniquement, en secret etc.

Il s'agit plus précisément:

— de la pénétration dans un domicile, lieu privé ou système informatique.

Cela permettra par exemple aux services de police de s'introduire dans un lieu déterminé, même s'il est sécurisé par des serrures, des systèmes d'alarme, etc., afin d'installer un dispositif d'écoute dans ce lieu.

Het heimelijk binnendringen in een woning of private plaats is in het huidig recht reeds mogelijk om direct afluisteren mogelijk te maken, maar is nieuw om de zoeking in een informaticasysteem mogelijk te maken;

— het tijdelijk (zo lang als nodig) opheffen van elke beveiliging van de informaticasystemen die geviseerd worden, desgevallend met behulp van technische hulpmiddelen, valse signalen, valse sleutels of valse hoedanigheden.

Net zoals dit het geval is bij de regeling in artikel 39*bis* (zie *supra* de toelichting bij dit artikel), worden onder het begrip "valse sleutels" ook vingerafdrukken en andere biometrische gegevens begrepen. Dit laat politiediensten toe een vingerafdruk, bijvoorbeeld uit een databank, aan te wenden om zich toegang te verschaffen tot een informaticasysteem. Men denke in dit verband bijvoorbeeld aan smartphones die uitgerust zijn met vingerafdrukbeveiliging;

— Het aanbrengen van technische middelen in de informaticasystemen die geviseerd worden, teneinde de door dat systeem opgeslagen, verwerkte of doorgestuurde gegevens te ontcijferen en te decoderen.

Dit laat de opsporingsdiensten toe om toegang te verkrijgen, in verstaanbare vorm, tot de gegevens die zich in een informaticasysteem bevinden of die erdoor verwerkt of doorgestuurd zijn.

De twee laatstgenoemde mogelijkheden staan niet enkel open voor de zoeking in een informaticasysteem, maar kunnen eveneens worden bevolen om een "klassieke" telefoontap of direct afluisteren te kunnen uitvoeren.

Teneinde de heimelijke zoeking in een informaticasysteem mogelijk te maken, zal het inderdaad soms noodzakelijk zijn om eerst buiten medeweten of zonder toestemming van de bewoner, de eigenaar of zijn rechthebbenden in een woning of private plaats binnen te dringen.

Bepaalde technologie maakt het mogelijk dat de politiediensten van op afstand binnendringen in een informaticasysteem om daarvan de gegevens te kopieren. Dit is echter niet altijd mogelijk. Bij sterk beveiligde computers zal het soms nodig zijn om binnen te dringen in de woning van de gebruiker ervan om een technisch middel te installeren waardoor de beveiliging kan omzeild worden, waarna de gegevens dan ter plekke gekopieerd kunnen worden.

La pénétration en secret dans un domicile ou un lieu privé est déjà possible dans le droit actuel pour permettre des écoutes directes, mais constitue une nouveauté pour permettre la recherche dans un système informatique;

— de la suppression temporaire (aussi longtemps que nécessaire) de toute protection des systèmes informatiques visés, le cas échéant à l'aide de moyens techniques, de faux signaux, de fausses clés ou de fausses qualités.

Comme c'est le cas pour le règlement prévu à l'article 39*bis* (voir plus haut commentaire de cet article), la notion de "fausses clés" comprend également les empreintes digitales et d'autres données biométriques.Cela permet aux services de police d'utiliser une empreinte digitale, provenant par exemple d'une banque de données, pour s'introduire dans un système informatique. Pensons par exemple à cet égard aux smartphones équipés d'une protection par empreinte digitale;

— de l'installation de dispositifs techniques dans les systèmes informatiques visés, en vue du décryptage et du décodage des données stockées, traitées ou transmises par ce système.

Cela permet aux services de recherche d'obtenir un accès, sous une forme compréhensible, aux données qui se trouvent dans un système informatique ou qui sont traitées ou transmises par ce système informatique.

Ces deux dernières possibilités ne s'ouvrent pas seulement pour la recherche dans un système informatique, elles peuvent également être ordonnées pour pouvoir exécuter des écoutes téléphoniques ou des écoutes directes "classiques".

Afin de permettre la recherche en secret dans un système informatique, il sera effectivement parfois nécessaire de pénétrer dans un domicile ou dans un lieu privé à l'insu ou sans le consentement de l'occupant, du propriétaire ou de ses ayants droit.

Une certaine technologie permet aux services de police d'accéder à distance à un système informatique afin d'en copier les données. Ce n'est toutefois pas toujours possible. Dans le cas d'ordinateurs fortement protégés, il sera parfois nécessaire de pénétrer dans le domicile de leur utilisateur afin d'installer un dispositif technique permettant de contourner la protection et de copier ensuite les données sur place.

Deze maatregel is tevens gebaseerd op de inkijkoperatie zoals die geregeld is door de artikelen 46*quinquies* en 89*ter* Sv. Er moet uiteraard aan dezelfde voorwaarden van proportionaliteit en subsidiariteit voldaan zijn als in het eerste lid. Het voorontwerp houdt daarbij dus rekening met de uitgebreide rechtspraak van het Grondwettelijk Hof en het Hof van Cassatie over de bescherming van de woning, zoals uitgebreid werd toegelicht in de Memorie van Toelichting bij de wet van 27 december 2005 (*Parl. St.*, Kamer, 2005-2006, 51-2055/001, p. 15-21).

Het moet echter onderstreept worden dat het voorontwerp strenger is dan de regeling betreffende de inkijkoperatie en voorziet dat zowel voor de private plaats, als voor de woning of de door een woning omsloten eigen aanhorigheid, steeds een machtiging van een onderzoeksrechter vereist is. Dit gaat inderdaad verder dan bij de inkijkoperatie, aangezien de inkijkoperatie in een private plaats door de procureur des Konings bevolen kan worden op basis van artikel 46*quinquies* Sv. Het voorontwerp houdt hier rekening met het ingrijpende karakter van de maatregel: het binnendringen in de woning is slechts een eerste stap om daarna een heimelijke zoeking in een informaticasysteem mogelijk te maken. Zoals voor alle onderzoeksmaatregelen die een dergelijke verregaande inbreuk op de persoonlijke levenssfeer tot gevolg hebben, kan enkel een onderzoeksrechter hiervoor bevoegd zijn.

Het doel van de heimelijke zoeking is om toegang te krijgen tot een informaticasysteem en er desgevallend de relevante gegevens van te kopiëren. De onderzoekers hebben daarvoor een maand de tijd: dat wil zeggen dat ze verschillende pogingen kunnen ondernemen om bijvoorbeeld een technisch middel te plaatsen, of dat ze het tijdstip kunnen bepalen wanneer er gegevens in beslag worden genomen, en dat ze ook over de nodige tijd beschikken om eventueel het technisch middel terug te gaan halen. De onderzoekers kunnen eveneens gedurende een bepaalde of de volledige periode van de machtiging een informaticasysteem “monitoren”, al dan niet gepaard gaande met continue of occasionele kopiename van de gegevens.

De onderzoekshandeling van de heimelijke zoeking in een informaticasysteem is een onderzoeksmaatregel die rekening houdt, enerzijds, met de (virtuele) realiteit van het internet en de daarop gangbare communicatievormen, doch ook anderzijds, met de realiteit en haalbaarheid van het rechercheren in dergelijke geïnformatiseerde omgeving. De wijze waarop de geheime netwerkzoeking wordt uitgevoerd zal in de praktijk vaak afhangen van de geïnformatiseerde omgeving die *in concreto* het voorwerp uitmaakt van de geheime

Cette mesure se fonde également sur la mesure du contrôle visuel discret, régie par les articles 46*quinquies* et 89*ter* du Code d’instruction criminelle. Il convient évidemment de répondre aux mêmes conditions de proportionnalité et de subsidiarité que dans l’alinéa 1er. À cet égard, l’avant-projet prend donc en considération l’abondante jurisprudence de la Cour constitutionnelle et de la Cour de cassation concernant la protection du domicile, telle que commentée de façon détaillée dans l’exposé des motifs de la loi du 27 décembre 2005 (*Doc. parl.*, Chambre, 2005-2006, 51-2055/001, pp. 15-21).

Il convient toutefois de souligner que l’avant-projet est plus strict que la réglementation relative au contrôle visuel discret et prévoit qu’une autorisation du juge d’instruction est toujours requise, tant pour le lieu privé que pour le domicile ou les dépendances propres y encloses. Cela va effectivement au-delà de ce qui est prévu pour le contrôle visuel discret vu que pour un lieu privé, celui-ci peut être ordonné par le procureur du Roi sur la base de l’article 46*quinquies* du Code d’instruction criminelle. L’avant-projet tient compte ici du caractère intrusif de la mesure: la pénétration dans le domicile n’est qu’une première étape pour permettre ensuite une recherche en secret dans un système informatique. Comme pour toutes les mesures d’instruction qui entraînent une atteinte aussi importante à la vie privée, seul un juge d’instruction peut être compétent.

L’objectif de la recherche en secret est d’accéder à un système informatique et éventuellement d’en copier les données pertinentes. Les enquêteurs disposent pour ce faire d’un mois: cela signifie qu’ils peuvent effectuer plusieurs tentatives afin de mettre en place un moyen technique, par exemple, ou qu’ils peuvent déterminer le moment où les données sont saisies et qu’ils disposent également du temps nécessaire pour éventuellement récupérer le moyen technique. Pendant une période déterminée ou la période complète de l’autorisation, les enquêteurs peuvent également “contrôler” un système informatique, avec ou sans prise de copie continue ou occasionnelle des données.

L’acte d’instruction de la recherche en secret dans un système informatique est une mesure d’enquête qui tient compte, d’une part, de la réalité (virtuelle) d’Internet et des formes de communication courantes sur celui-ci, mais également, d’autre part, de la réalité et de la faisabilité de la recherche dans un tel environnement informatisé. Dans la pratique, la manière dont s’effectuera la recherche en secret sur réseau dépendra souvent de l’environnement informatisé qui fait *in concreto* l’objet de la recherche en secret sur réseau. Ainsi, il est

netwerkzoeking. Zo is het denkbaar dat er door de politiediensten van op afstand – onder dekking van een strikt afgelijnd mandaat van de onderzoeksrechter – éénmalig wordt ingebroken in een informaticasysteem waarbij bepaalde data zal worden gekopieerd. Het is echter ook denkbaar dat er heimelijk een drager (harde schijf, USB, …) rechtstreeks zou worden gekoppeld aan het te doorzoeken informaticasysteem, waarbij alle data gedurende een bepaalde tijdspanne wordt gekopieerd, om vervolgens nadien het voorwerp uit te maken van een analyse en exploitatie door de politiediensten.

Het is daarbij niet uit te sluiten dat er data worden gekopieerd of overgenomen waarvan niet geweten is of deze (nog) in transmissie zijn. Het huidig artikel biedt, zoals reeds eerder aangehaald, een duidelijke rechtsgrond om daarin geen onderscheid te maken. Met andere woorden, in het kader van de heimelijke zoeking in een informaticasysteem kunnen data gekopieerd worden ongeacht in welke doorsturingsfase deze zich zouden bevinden.

LID 4:

De toevoeging aan het vierde lid van artikel 90*ter*, § 1 van het Wetboek van strafvordering in ontwerp is een verdere inperking van de maatregel bedoeld in dit artikel, maar eveneens een verduidelijking van de huidige toestand. De maatregel zal enkel bevolen kunnen worden om de gegevens op te sporen die kunnen dienen om de waarheid aan de dag te brengen. Dit betekent dat “verkennende” zoekingen in informaticasystemen niet mogelijk zijn.

Het gebeurt vaak dat een verdachte niet zijn eigen computer gebruikt om het misdrijf te plegen, maar de computer van een ander persoon, soms zelfs zonder diens medeweten. Vandaar dat het mogelijk moet zijn om ook bij deze andere persoon een zoeking uit te voeren. Het kan daarbij uiteraard niet gaan over om het even wie: men moet telkens over voldoende en precieze aanwijzingen beschikken dat, bijvoorbeeld, de verdachte op bepaalde plaatsen verblijft, van bepaalde informaticasystemen gebruik maakt, of geregeld in verbinding staat met deze andere personen. Het doel is met andere woorden om te kunnen nagaan in hoeverre een verdachte gebruik maakt van andere informaticasystemen. De gerechtelijke finaliteit blijft vooropstaan: de heimelijke zoeking in een informaticasysteem kan enkel worden bevolen om de gegevens op te sporen die kunnen dienen om de waarheid aan de dag te brengen. Naar analogie met de huiszoeking wordt deze finaliteit expliciet in dit vierde lid vermeld.

envisageable que les services de police pénètrent en une seule occasion à distance – sous le couvert d’un mandat strictement défini du juge d’instruction – dans un système informatique et que certaines données soient copiées. Toutefois, il est également envisageable qu’un support (disque dur, clé USB, etc.) soit connecté directement en secret au système informatique à explorer et que toutes les données soient copiées pendant un laps de temps déterminé, pour ensuite être analysées et exploitées par les services de police.

Il n’est en outre pas exclu que des données dont on ne sait pas si elles sont (encore) en transmission soient copiées ou reprises. Comme déjà indiqué, l’article actuel offre un fondement juridique clair pour ne pas faire de distinction à ce sujet. En d’autres termes, dans le cadre de la recherche en secret dans un système informatique, des données peuvent être copiées quel que soit leur stade de transmission.

ALINÉA 4:

L’ajout effectué à l’alinéa 4 de l’article 90*ter*, § 1er, du Code d’instruction criminelle, en projet constitue une limitation supplémentaire de la mesure visée à cet article, mais également une précision quant à la situation actuelle. La mesure ne pourra uniquement être ordonnée qu’afin de rechercher les données pouvant servir à la manifestation de la vérité. Cela signifie que des recherches “exploratoires” dans des systèmes informatiques ne sont pas possibles.

Il est fréquent qu’un suspect n’utilise pas son propre ordinateur pour commettre l’infraction mais l’ordinateur d’une autre personne, parfois même à son insu. Il doit donc être possible d’effectuer une recherche chez cette autre personne également. Il ne peut évidemment pas s’agir de n’importe qui: il faut à chaque fois disposer d’indices suffisants et précis selon lesquels par exemple le suspect séjourne à certains endroits, utilise certains systèmes informatiques ou est régulièrement en relation avec ces autres personnes. En d’autres termes, l’objectif est de pouvoir vérifier dans quelle mesure un suspect utilise d’autres systèmes informatiques. La finalité judiciaire reste primordiale: la recherche en secret dans un système informatique ne peut être ordonnée qu’aux fins de rechercher les données susceptibles d’être utiles à la manifestation de la vérité. Par analogie avec la perquisition, cette finalité est explicitement mentionnée dans cet alinéa 4.

§ 2. LIJST

Er werd geopteerd voor een hernummering van de lijst met misdrijven waarvoor een tap mogelijk is, omdat dit de leesbaarheid verhoogt.

Daarnaast zijn enkele nieuwe misdrijven aan de lijst toegevoegd. Het gaat meer bepaald om de volgende misdrijven:

— Artikel 147 van hetzelfde Wetboek (wederrechtelijke vrijheidsberoving door ambtenaar)

(Onderstaande motivering geldt evenzeer voor artikel 434 Sv.)

Het onderscheid tussen een gijzeling (artikel 347*bis* Sw. – momenteel reeds opgenomen in de lijst) en een wederrechtelijke vrijheidsberoving is in de praktijk niet altijd duidelijk, zeker niet op het moment dat de feiten zich nog afspelen. De gijzeling veronderstelt immers dat iemand wordt aangehouden, gevangengenomen of ontvoerd "om deze borg te doen staan voor de voldoening aan een bevel of een voorwaarde". Bij gebrek aan dit bijzonder opzet zijn eventueel de strafbepalingen betreffende de wederrechtelijke aanhouding, gevangenhouding of ontvoering toepasselijk.

Politie en parket (voornamelijk de zogenaamde "BOM-magistraten") worden in de praktijk geconfronteerd met feiten waarbij het niet onmiddellijk duidelijk is of het om een "gijzeling" gaat, dan wel een zuivere "wederrechtelijke vrijheidsberoving" (ontvoering) - waarbij dus *ab initio* geen bevel of voorwaarde werd gesteld. Niettemin zijn dit vaak dossiers waarbij de fysieke integriteit van het ontvoerde slachtoffer minstens evenzeer wordt bedreigd als bij een gijzeling in bijvoorbeeld het zwaardere criminele milieu en derhalve een zeer snelle en effectieve tussenkomst vereisen.

In de praktijk gaat het bijvoorbeeld om:

— ontvoering van minderjarige kinderen zonder dat geweten is om welke reden en met welke bedoeling het kind ontvoerd wordt;

— ontvoeringen van jonge meisjes, bv. om deze een gedwongen huwelijk te laten sluiten of in de prostitutie te laten belanden;

— ontvoering van vrouwen binnen een relationele context;

— ontvoeringen in het criminele milieu waarbij niet onmiddellijk een bevel of voorwaarde wordt geuit (bv.

§ 2. LISTE

Il a été décidé de renuméroter la liste des infractions pouvant faire l'objet d'une écoute parce que cela améliore la lisibilité.

En outre, quelques nouvelles infractions sont ajoutées à la liste. Il s'agit plus particulièrement des infractions suivantes:

— Article 147 du même Code (détention illégale par fonctionnaire)

(la motivation ci-dessous s'applique également à l'article 434 du Code d'instruction criminelle)

La différence entre une prise d'otage (article 347*bis* du Code pénal – qui figure déjà dans la liste) et une détention illégale n'est pas toujours claire en pratique, et assurément pas au moment où les faits sont toujours en cours. La prise d'otage suppose en effet que quelqu'un est arrêté, détenu ou enlevé "pour répondre de l'exécution d'un ordre ou d'une condition". En l'absence de cette intention spécifique, les dispositions pénales relatives à la détention illégale, à la détention ou à l'enlèvement sont éventuellement d'application.

Dans la pratique, la police et le parquet (essentiellement les "magistrats MPR") sont confrontés à des faits dont il ne ressort pas immédiatement de façon claire s'ils concernent une "prise d'otage" ou une "détention illégale" (enlèvement) pure et simple n'ayant donc fait l'objet *ab initio* d'aucun ordre ou d'aucune condition. Il s'agit toutefois souvent de dossiers où l'intégrité physique de la victime enlevée est au moins aussi menacée que dans le cas d'une prise d'otage, par exemple dans le milieu criminel, nécessitant par conséquent une intervention très rapide et efficace.

Il s'agit dans la pratique, par exemple, des faits suivants:

— enlèvement d'enfants mineurs sans que l'on sache pour quelle raison et dans quel but l'enfant a été enlevé;

— enlèvements de jeunes filles, p. ex. pour les marier de force ou les faire entrer dans la prostitution;

— enlèvement de femmes dans un contexte relationnel;

— enlèvements dans le milieu criminel pour lesquels il n'est pas exprimé immédiatement d'ordre ou de

iemand wordt ontvoerd door mannen die genoegzaam gekend zijn in het drugmilieu en er wordt niet onmiddellijk een bevel of voorwaarde geuit door de verdachten).

In deze gevallen wordt de fysieke integriteit van de ontvoerde slachtoffers zeer ernstig bedreigd en dringt er zich een zeer snelle tussenkomst op van politie en justitie. Telefoniemaatregelen (afluisteren) zijn vaak de enige nuttige onderzoeksmogelijkheden om een snelle inschatting van de gevaarsituatie te kunnen maken. Het is niet te rechtvaardigen dat er wettelijk gezien een onderscheid wordt gemaakt tussen, enerzijds, de slachtoffers die zich in de meeste gevallen volledig buiten enig crimineel milieu situeren (zeker de kinderen) en die ontvoerd worden met een ander opzet dan het verkrijgen van losgeld, en anderzijds de slachtoffers (in de praktijk zelf ook vaak criminelen of personen met criminele achtergrond) die gegijzeld worden.

Deze leemte werd opgemerkt door de procureur-generaal bij het Hof van Cassatie in het verslag 2013-2014 van het Parlementair Comité belast met de wetsevaluatie (DOC 54 0435/001, blz. 28).

Een uitbreiding van de lijst van artikel 90*ter*, § 2, met de artikelen 147 en 434 Sw. dringt zich dan ook op.

— De artikelen 160, 161, 162, 163, 168, 171, 173 en 176 van hetzelfde Wetboek (valsemunterij)

De toevoeging van deze artikelen kadert in de omzetting van de Richtlijn 2014/62/EU van 15 mei 2014 betreffende de strafrechtelijke bescherming van de Euro en andere munten tegen valsemunterij en ter vervanging van Kaderbesluit 2000/383/JBZ.

Artikel 9 betreft de onderzoeksbevoegdheden en bepaalt dat de lidstaten de nodige maatregelen nemen om ervoor te zorgen dat doeltreffende onderzoeksbevoegdheden, zoals die welke worden gebruikt bij georganiseerde of andere zware criminaliteit, ter beschikking staan van personen, eenheden of diensten die bevoegd zijn voor het onderzoeken of vervolgen van de in de artikelen 3 en 4 genoemde strafbare feiten.

Overweging (21) specifieert dat om gevallen van valsemunterij naar behoren te kunnen onderzoeken en juridisch te kunnen vervolgen, diegenen die dergelijke gevallen onderzoeken en vervolgen, de mogelijkheid moeten hebben om gebruik te maken van doeltreffende onderzoeksmiddelen, zoals die welke worden gebruikt bij de bestrijding van georganiseerde misdaad of andere ernstige misdaden. Deze middelen zouden in voorkomend geval kunnen bestaan uit het aftappen van communicatie, het – ook elektronisch – schaduwen

condition (p. ex. quelqu'un est enlevé par des hommes suffisamment connus dans le milieu et aucun ordre ou aucune condition n'est immédiatement exprimé par les suspects).

Dans de tels cas, l'intégrité physique des victimes enlevées est très fortement menacée et une intervention très rapide de la police et de la justice s'impose. Les mesures en matière de téléphonie (écoutes) sont souvent les seules possibilités d'investigation possibles pour pouvoir évaluer rapidement la situation de danger. On ne peut justifier l'établissement d'une distinction sur le plan légal entre, d'une part, les victimes qui sont dans la plupart des cas étrangères à tout milieu criminel (ce qui est certainement le cas des enfants) et qui sont enlevées dans un autre but que l'obtention d'une rançon et, d'autre part, les victimes (qui dans la pratique sont souvent aussi des criminels ou des personnes au passé criminel) qui sont prises en otage.

Cette lacune a été épinglée par le procureur général près la Cour de cassation dans le rapport 2013-2014 du Comité parlementaire chargé du suivi législatif (DOC 54 435/001, p. 28).

Une extension de la liste de l'article 90*ter*, § 2, aux articles 147 et 434 du Code pénal s'impose dès lors.

— Articles 160, 161, 162, 163, 168 171, 173 et 176 du même Code (fausse monnaie)

L'ajout de ces articles s'inscrit dans le cadre de la transposition de la Directive 2014/62/UE du 15 mai 2014 relative à la protection pénale de l'euro et des autres monnaies contre la contrefaçon et remplaçant la décision-cadre 2000/383/JAI du Conseil.

L'article 9 traite des outils d'enquête et prévoit que les États membres prennent les mesures nécessaires pour que des outils d'enquête efficaces, tels que ceux qui sont utilisés dans les affaires de criminalité organisée ou d'autres formes graves de criminalité, soient mis à la disposition des personnes, des unités ou des services chargés des enquêtes ou des poursuites concernant les infractions visées aux articles 3 et 4.

Le considérant 21 précise qu'afin d'assurer la réussite des enquêtes et des poursuites relatives à des infractions de faux monnayage, les personnes chargées de ces enquêtes et de ces poursuites devraient avoir la possibilité de recourir à des outils d'investigation performants tels que ceux utilisés dans la lutte contre la criminalité organisée ou d'autres formes graves de criminalité. Ces outils pourraient comprendre, le cas échéant, par exemple, l'interception de communications, la surveillance discrète, y compris la surveillance

van personen, het controleren van bankrekeningen en andere vormen van financieel onderzoek.

De voornoemde artikelen van het Strafwetboek en deze in het volgende punt vallen allemaal onder de artikelen 3 en 4 van de Richtlijn.

— De artikelen 180 en 186 van hetzelfde Wetboek (valsemunterij)

De toevoeging van deze artikelen kadert eveneens in de omzetting van de Richtlijn 2014/62/EU van 15 mei 2014 betreffende de strafrechtelijke bescherming van de Euro en andere munten tegen valsemunterij en ter vervanging van Kaderbesluit 2000/383/JBZ.

Zie *supra* voor verdere toelichting.

— De artikelen 372 tot 377*bis* van hetzelfde Wetboek (verkrachting)

In het reeds genoemde verslag 2013-2014 van het Parlementair Comité belast met de wetsevaluatie (DOC 54 K 0435/001, blz. 28) wijst de procureur-generaal er op dat het hoogst wenselijk zou zijn om ook voor de misdrijven van aanranding van de eerbaarheid en verkrachting een afluistermaatregel te wettigen. Het bewijs van dergelijke feiten is vaak delicaat en moeilijk en komt in de praktijk vaak neer op een verhaal van woord en wederwoord tussen twee partijen. Aangezien de andere middelen van onderzoek niet altijd zullen volstaan om de waarheid aan de dag te brengen, kan een telefoontap hier nodig zijn.

— Artikel 377*quater* van hetzelfde Wetboek (grooming)

De toevoeging van dit artikel kadert in de omzetting van de Richtlijn 2011/93/EU van het Europees Parlement en de Raad van 13 december 2011 ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie, en ter vervanging van Kaderbesluit 2004/68/JBZ van de Raad.

Artikel 15.3 van deze Richtlijn bepaalt dat de lidstaten de nodige maatregelen nemen om ervoor te zorgen dat doeltreffende onderzoekmiddelen, zoals die welke worden gebruikt bij georganiseerde of andere zware criminaliteit, ter beschikking staan van personen, eenheden of diensten die bevoegd zijn voor het onderzoeken of vervolgen van de in de artikelen 3 tot en met 7 genoemde strafbare feiten. Artikel 6 van de Richtlijn betreft grooming. In overweging 27 wordt uitgelegd dat het daarbij kan gaan over onder meer het onderscheppen van gesprekken, geheime observatie, onder meer met elektronische middelen, toezicht op bankrekeningen of andere financiële onderzoeken, daarbij rekening

électronique, la surveillance de comptes bancaires et d'autres enquêtes financières.

Les articles précités du Code pénal et ceux figurant dans le point suivant tombent sous l'application des articles 3 et 4 de la directive.

— Articles 180 et 186 du même Code (fausse monnaie)

L'ajout de ces articles s'inscrit également dans le cadre de la transposition de la Directive 2014/62/UE du 15 mai 2014 relative à la protection pénale de l'euro et des autres monnaies contre la contrefaçon et remplaçant la décision-cadre 2000/383/JAI du Conseil.

Voir *supra* pour plus d'explications.

— Articles 372 à 377*bis* du même Code (viol)

Dans le rapport 2013-2014 du Comité parlementaire chargé du suivi législatif (DOC 54 0435/001, p. 28), déjà mentionné, le procureur général souligne qu'il serait hautement souhaitable que la loi autorise également la prise de mesures de surveillance téléphonique pour les attentats à la pudeur et les viols. La question des preuves, pour de tels faits, est souvent délicate, et, dans la pratique, c'est souvent la parole d'une partie contre celle de l'autre. Comme les autres moyens d'enquête ne suffiront pas toujours pour établir la vérité, une écoute téléphonique peut être un moyen nécessaire pour résoudre cette difficulté.

— Article 377*quater* du même Code (grooming)

L'ajout de cet article s'inscrit dans la transposition de la Directive 2011/93/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil.

L'article 15.3 de cette directive prévoit que les États membres prennent les mesures nécessaires pour que des outils d'investigation efficaces, tels que ceux qui sont utilisés dans les affaires de criminalité organisée ou d'autres formes graves de criminalité, soient mis à la disposition des personnes, des unités ou des services chargés des enquêtes ou des poursuites concernant les infractions visées aux articles 3 à 7. L'article 6 de la directive traite du grooming. Le considérant 27 explique que ces moyens pourraient comprendre l'interception de communications, la surveillance discrète, notamment électronique, la surveillance de comptes bancaires, ou d'autres enquêtes financières, compte tenu notamment

houdend met, onder andere, het evenredigheidsbeginsel en de aard en ernst van de onderzochte strafbare feiten.

— De artikelen 379, 380 en 383*bis*, § 1 en § 3 van hetzelfde Wetboek (kinderpornografie)

Dit artikel kadert eveneens in de omzetting van de Richtlijn 2011/93/EU van het Europees Parlement en de Raad van 13 december 2011 ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie, en ter vervanging van Kaderbesluit 2004/68/JBZ van de Raad.

Zie *supra* voor verdere toelichting. Artikel 5 van de Richtlijn betreft kinderpornografie.

— Artikel 433*bis*/1 van hetzelfde Wetboek

Dit artikel kadert eveneens in de omzetting van de Richtlijn 2011/93/EU van het Europees Parlement en de Raad van 13 december 2011 ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie, en ter vervanging van Kaderbesluit 2004/68/JBZ van de Raad.

Zie *supra* voor verdere toelichting.

— De artikelen 433*quinquies* tot 433*octies* van hetzelfde Wetboek (mensenhandel)

De invoeging van dit artikel kadert in de omzetting van de Richtlijn 2011/36/EU van het Europees Parlement en de Raad van 5 april 2011 inzake de voorkoming en bestrijding van mensenhandel en de bescherming van slachtoffers daarvan, en ter vervanging van Kaderbesluit 2002/629/JBZ van de Raad.

Artikel 9.4 van deze Richtlijn bepaalt dat de lidstaten de nodige maatregelen nemen om ervoor te zorgen dat personen, eenheden en diensten die zijn belast met het onderzoek of de vervolging betreffende de in de artikelen 2 en 3 bedoelde strafbare feiten, beschikken over doeltreffende recherchemiddelen, zoals die welke ter zake van georganiseerde en andere zware criminaliteit worden gebruikt.

Overweging 15 preciseert dat de personen belast met het onderzoek naar en de vervolging van dergelijke strafbare feiten, moeten middelen ter beschikking hebben die bij de bestrijding van georganiseerde en andere zware criminaliteit worden gebruikt. Deze middelen kunnen bestaan uit het aftappen van communicatie, het – ook elektronisch – schaduwen van personen, het controleren van bankrekeningen en andere vormen van financieel onderzoek.

du principe de proportionnalité et de la nature et de la gravité des infractions faisant l'objet de l'enquête.

— Articles 379, 380 et 383*bis*, §§ 1er et 3, du même Code (pornographie infantile)

Cet article s'inscrit également dans la transposition de la Directive 2011/93/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil.

Voir *supra* pour plus d'explications. L'article 5 de la directive traite de la pédopornographie.

— Article 433*bis*/1 du même Code

Cet article s'inscrit également dans la transposition de la Directive 2011/93/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil.

Voir *supra* pour plus d'explications.

— Articles 433*quinquies* à 433*octies* du même Code (traite des êtres humains)

2011/36/UE du Parlement européen et du Conseil du 5 avril 2011 concernant la prévention de la traite des êtres humains et la lutte contre ce phénomène ainsi que la protection des victimes et remplaçant la décision-cadre 2002/629/JAI du Conseil.

L'article 9.4 de cette directive prévoit que les États membres prennent les mesures nécessaires pour que des outils d'investigation efficaces, tels que ceux qui sont utilisés dans les affaires de criminalité organisée ou d'autres formes graves de criminalité, soient mis à la disposition des personnes, des unités ou des services chargés des enquêtes ou des poursuites concernant les infractions visées aux articles 2 et 3.

Le considérant 15 précise que les personnes chargées des enquêtes ou des poursuites concernant ces infractions devraient aussi avoir accès aux outils d'investigation utilisés dans les affaires relatives à la criminalité organisée ou à d'autres formes graves de criminalité. Ces outils pourraient comprendre l'interception des communications, la surveillance discrète, y compris électronique, la surveillance des comptes bancaires ou autres investigations financières.

Artikel 2 van de Richtlijn omvat ook de poging tot mensenhandel. Dit is opgenomen in artikel 433*quinquies* van het Strafwetboek.

De werkgroep die instond voor de omzetting van deze Richtlijn heeft er ook op gewezen dat er een incoherentie bestond in artikel 90*ter*. Er wordt nu namelijk wel verwezen naar prostitutie zonder verzwarende omstandigheden, maar voor mensenhandel was er enkel een tap mogelijk als het om mensenhandel met verzwarende omstandigheden ging. De toevoeging van artikel 433*quinquies* van het Strafwetboek aan de "taplijst" maakt het mogelijk dat de tap en heimelijke zoeking ook kunnen worden bevolen bij onderzoeken naar mensenhandel zonder verzwarende omstandidgheden.

— Artikel 434 van hetzelfde Wetboek (wederrechtelijke vrijheidsberoving)

Zelfde motivering als voor artikel 147 Sw. (zie *supra*).

— Artikel 505, eerste lid, 1° van hetzelfde Wetboek (heling)

Op dit moment zijn de punten 2°, 3° en 4° van artikel 505, eerste lid, reeds opgenomen in de lijst van artikel 90*ter*, § 2. Deze slaan allen op verrichtingen met betrekking tot zaken die uit een misdrijf voortkomen, zoals witwassen.

Punt 1°, dat het misdrijf "heling" omschrijft, ligt geheel in dezelfde lijn. De toevoeging van dit misdrijf aan de "taplijst" is dan ook een logische uitbreiding, die het mogelijk zal maken de maatregel van artikel 90*ter*, § 1, ook toe te passen ten aanzien van helers. Zo zullen de opsporingsdiensten bijvoorbeeld de privécommunicatie kunnen afluisteren van kunstrovers die hun gestolen goederen via het zwarte circuit proberen te verkopen. Dit zal echter alleen mogelijk zijn wanneer de betrokken zaken werden weggenomen, verduisterd of verkregen door een misdaad of wanbedrijf vermeld in de lijst van artikel 90*ter*, § 2.

— Artikel 2*bis* van de wet van 24 februari 1921 betreffende het verhandelen van giftstoffen, slaapmiddelen en verdovende middelen, psychotrope stoffen, ontsmettingsstoffen en antiseptica en van de stoffen die kunnen gebruikt worden voor de illegale vervaardiging van verdovende middelen en psychotrope stoffen

Deze wijziging beoogt slechts het opschrift van de wet van 24 februari 1921 aan te passen zoals dit is gebeurd door de wet van 3 mei 2003 tot wijziging van de wet van 24 februari 1921 betreffende het verhandelen van

L'article 2 de la directive traite également de la tentative de traite des êtres humains. Celle-ci figure à l'article 433*quinquies* du Code pénal.

Le groupe de travail en charge de la transposition de cette directive a également souligné l'existence d'une incohérence à l'article 90*ter*. Actuellement, il est renvoyé à la prostitution sans circonstances aggravantes, mais pour la traite des êtres humains, une écoute téléphonique n'était possible que si elle s'accompagnait de circonstances aggravantes. L'ajout de l'article 433*quinquies* du Code pénal à la "liste des écoutes" permet d'ordonner également des écoutes et une recherche en secret dans des enquêtes en matière de traite des êtres humains sans circonstances aggravantes.

— Article 434 du même Code (détention illégale)

Même motivation que pour l'article 147 du Code pénal. (voir *supra*).

— Article 505, alinéa 1er, 1°, du même Code (recèlement)

Actuellement, les 2°, 3° et 4° de l'article 505, alinéa 1er, figurent déjà dans la liste de l'article 90*ter*, § 2. Ils ne portent que sur des opérations relatives à des choses tirées d'une infraction, comme le blanchiment.

Le 1°, qui définit le "recèlement", s'inscrit tout à fait dans la même lignée. L'ajout de cette infraction à la "liste des écoutes" constitue dès lors une extension logique qui permettra également d'appliquer la mesure de l'article 90*ter*, § 1er, aux receleurs. Ainsi, les services de recherche pourront, par exemple, écouter des communications privées de voleurs d'œuvres d'art qui tentent de vendre les biens qu'ils ont volés sur le circuit parallèle. Ceci ne sera que possible lorsque les choses concernées ont été enlevées, détournées ou obtenues à l'aide d'un crime ou d'un délit visé dans la liste de l'article 90*ter*, § 2.

— Article 2*bis* de la loi du 24 février 1921 concernant le trafic des substances vénéneuses, soporifiques, stupéfiantes, psychotropes, désinfectantes ou antiseptiques et des substances pouvant servir à la fabrication illicite de substances stupéfiantes et psychotropes

Cette modification vise uniquement l'adaptation de l'intitulé de la loi du 24 février 1921 comme ce fut le cas par la loi du 3 mai 2003 modifiant la loi du 24 février 1921 concernant le trafic des substances

de giftstoffen, slaapmiddelen en verdovende middelen, ontsmettingsstoffen en antiseptica (*BS* 2 juni 2003).

— De artikelen 77*bis* tot 77*quinquies* van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen.

De mogelijkheid om de maatregelen van artikel 90*ter*, § 1 in te zetten, zal worden uitgebreid tot de gevallen van mensensmokkel zonder aanwezigheid van verzwarende omstandigheden, om de bestaande parallellie tussen mensenhandel en mensensmokkel te behouden. Tot nu toe is er namelijk altijd voor gekozen, omwille van de nauwe verbondenheid tussen deze misdrijven en gelet op de huidige vluchtelingencrisis, om de straffen voor mensenhandel en mensensmokkel op dezelfde hoogte te houden en om andere wijzigingen inzake mensenhandel ook door te trekken naar mensensmokkel. Aangezien, zoals hoger toegelicht, artikel 433*quinquies* Sw. (mensenhandel zonder verzwarende omstandigheden) in de "taplijst" wordt ingeschreven, wordt dit tevens gedaan voor artikel 77*bis* van de wet van 15 december 1980 (mensensmokkel zonder verzwarende omstandigheden).

De wijzigingen aan § 5 van artikel 90*ter* zijn tweeledig:

— Aanpassing van de Nederlandse versie van deze bepaling aan de Franse versie;

— Toevoeging van artikel 434 Sw. (wederrechtelijke vrijheidsberoving). Aangezien de toepassing van de maatregel van artikel 90*ter*, § 1, in de context van terrorisme of wederrechtelijke vrijheidsberoving vaak noodzakelijk is binnen een zeer korte tijdspanne, wordt de procureur des Konings de mogelijkheid gegeven om deze maatregel te bevelen wanneer het gaat om ontdekking op heterdaad.

In § 6 van artikel 90*ter* van het Wetboek van strafvordering wordt de vereiste dat inhoudsgegevens enkel geïntercepteerd mogen worden "tijdens de overbrenging ervan" geschrapt. (Zie ook motivering art. 90*ter*, § 1, eerste lid van het Wetboek van strafvordering)

Artikel 18

Artikel 18 vervangt artikel 90*quater* van het Wetboek van strafvordering.

vénéneuses, soporifiques, stupéfiantes, psychotropes, désinfectantes ou antiseptiques février 1921 (*MB* du 2 juin 2003).

— Articles 77*bis* à 77*quinquies* de la loi du 15 décembre 1980 concernant l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers.

La possibilité de mettre en œuvre les mesures de l'article 90*ter*, § 1er, sera étendue aux cas de trafic des êtres humains sans circonstances aggravantes, afin de maintenir le parallélisme existant entre la traite et le trafic des êtres humains. Jusqu'à présent, en raison de l'étroite relation existant entre ces infractions et compte tenu de la crise actuelle des réfugiés, on a toujours choisi de maintenir la traite et le trafic des êtres humains au même niveau et d'étendre d'autres modifications en matière de traite des êtres humains au trafic des êtres humains. Étant donné que, comme expliqué plus haut, l'article 433*quinquies* du Code pénal (traite des êtres humains sans circonstances aggravantes) est inscrit dans la "liste des écoutes", il en est de même pour l'article 77*bis* de la loi du 15 décembre 1980 (trafic des êtres humains sans circonstances aggravantes).

Les modifications apportées au § 5 de l'article 90*ter* sont doubles:

— Adaptation de la version néerlandaise de cette disposition à la version française;

— Ajout de l'article 434 (détention illégale) du Code pénal. Étant donné que l'application de la mesure de l'article 90*ter*, § 1er, est souvent nécessaire dans un très court laps de temps dans le contexte du terrorisme et de la détention illégale, le procureur du roi se voit offrir la possibilité d'ordonner cette mesure en cas de flagrant délit.

Au § 6 de l'article 90*ter* du Code d'instruction criminelle, l'exigence selon laquelle les données relatives au contenu ne peuvent être interceptées que "durant leur transmission" est supprimée. (Voir également la motivation de l'article 90*ter*, § 1er, alinéa 1er, du Code d'instruction criminelle).

Article 18

L'article 18 remplace l'article 90*quater* du Code d'instruction criminelle.

§ 1.

Het eerste lid van § 1 stelt dat de machtiging van de onderzoeksrechter inzake een maatregel op grond van art. 90*ter* van het Wetboek van strafvordering steeds schriftelijk, voorafgaand en met reden omkleed moet zijn.

In het tweede lid van § 1 worden een aantal vermeldingen opgesomd die de machtiging van de onderzoeksrechter dient te bevatten.

De vierde nodige vermelding is geherformuleerd. De periode tijdens dewelke de maatregel van artikel 90*ter* kan worden uitgeoefend, is nog steeds vastgelegd op een maand.

Daarnaast wordt verduidelijkt wanneer deze termijn begint te lopen en wanneer deze eindigt. Ingeval de onderzoeksrechter een mondelinge machtiging verleent op grond van artikel 90*quater*, § 1, derde lid, vangt de maximumtermijn van een maand aan op de dag van die mondelinge machtiging en niet op de dag van de schriftelijke bevestiging van de mondelinge machtiging.

Het nieuwe derde lid van § 1 voorziet dat de beschikking, die steeds schriftelijk gebeurt, in spoedeisende gevallen in een eerste fase ook mondeling kan worden verstrekt. Zij moet dan wel binnen 24 uren schriftelijk worden bevestigd, met opgave van alle wettelijk voorziene vermeldingen.

§ 2.

Paragraaf 2 wordt in dezelfde zin gewijzigd als artikel 46*bis* (zie de uitgebreide toelichting bij dit artikel). De term “verstrekker van een elektronische communicatiedienst” wordt vervangen door een nieuwe, ruimere omschrijving die overeenstemt met de interpretatie van het Hof van Cassatie in zijn “Yahoo-arrest” van 18/01/2011. Daarnaast wordt de termijn voor het verlenen van medewerking aangepast naar “in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering”.

Ook de strafmaat in deze paragraaf wordt gewijzigd, van een maximum geldboete van tienduizend frank naar twintigduizend frank. Dit om een gelijkschakeling door te voeren met § 4 van artikel 90*quater*. Hierin wordt voor personen, waarvan de onderzoeksrechter vermoedt dat ze een bijzondere kennis hebben en die hun technische medewerking weigeren, eveneens een geldboete van zesentwintig euro tot twintigduizend euro bepaald.

§ 1er.

L’alinéa 1er du § 1er précise qu’une mesure sur la base de l’article 90*ter* du Code d’instruction criminelle doit faire l’objet d’une autorisation préalable motivée du juge d’instruction.

L’alinéa 2 du § 1er énonce un certain nombre de mentions qui doivent être présentes dans cette autorisation du juge d’instruction.

La quatrième mention requise a été reformulée. La période pendant laquelle la mesure indiquée à l’article 90*ter* peut être pratiquée reste fixée à un mois.

Il est en outre précisé quand ce délai commence à courir et quand il prend fin. Si le juge d’instruction accorde une autorisation verbale sur la base de l’article 90*quater*, § 1er, alinéa 3, le délai maximal d’un mois commence le jour de cette autorisation verbale et non le jour de la confirmation écrite de l’autorisation verbale.

Le nouvel alinéa 3 du § 1er prévoit qu’en cas d’urgence, l’autorisation, qui doit toujours être formulée par écrit, peut également être donnée oralement dans un premier temps. Elle doit alors être confirmée par écrit au plus tard dans les 24 heures, en mentionnant tous les éléments prévus par la loi.

§ 2.

Le paragraphe 2 est modifié dans le même sens comme l’article 46*bis* (voir commentaire détaillé de cet article). Les termes “fournisseur d’un service de communications électroniques” sont remplacés par une nouvelle définition, plus large, conforme à l’interprétation de la Cour de cassation dans son “arrêt Yahoo” du 18/01/2011. En outre, le délai pour prêter sa collaboration est adapté et devient “en temps réel ou, le cas échéant, au moment précisé dans la réquisition”.

Le taux de la peine figurant dans ce paragraphe est également modifié pour passer d’une amende maximale de dix mille francs à une amende de vingt mille francs afin que cela concorde avec le § 4 de l’article 90*quater*. Ce paragraphe prévoit également une amende de vingt-six euros à vingt mille euros pour les personnes dont le juge d’instruction présume qu’elles ont une connaissance particulière et qui refusent de fournir leur collaboration technique.

Indien de strafmaat in § 2 niet zou worden aangepast, blijft er een niet te rechtvaardigen ongelijkheid bestaan tussen, enerzijds, operatoren, verstrekkers van elektronische communicatiediensten etc., en anderzijds andere personen die hun medewerking niet verlenen. Bovendien is de financiële draagkracht van eerstgenoemde categorie (lees: rechtspersonen) meestal veel groter dan die van natuurlijke personen.

§ 3.

Het is in de praktijk onmogelijk voor officieren en agenten van gerechtelijke politie om alle telefoontaps af te handelen (zeker wat het beluisteren en uittypen betreft). Daarom moeten ze een beroep kunnen doen op burgers die deze taken uitvoeren, de zogenaamde CaLog-personeelsleden. Het gaat hier niet om het openstellen van deze mogelijkheid aan gelijk welk lid van het CaLog-personeel. De precieze voorwaarden, in het bijzonder wat betreft vorming, zullen voorzien worden door de Koning.

Twee soorten taken kunnen in geen geval aan CaLog-personeelsleden overgelaten worden: de analyse van de inhoud van de opgenomen communicatie of gegevens en de selectie van relevante delen. CaLog-personeelsleden kunnen echter wel de inhoud van bepaalde opnames analyseren indien het om een specifieke expertise gaat.

Concreet voorbeeld: in geval van “IP-taps” kan het, omwille van de complexiteit van de technische gegevens die verzameld zijn, nodig zijn om goed opgeleid technisch CaLog-personeel in te schakelen om die gegevens te ordenen, pre-analyseren etc.

Enkele taken die aan CaLog-personeel kunnen worden toevertrouwd:

— Beluisteren en uitschrijven van telefoontaps;

— Helpen bij de vertaling;

— Administratieve taken: gegevens archiveren en dergelijke.

In plaats van de namen van de personen die aan het dossier werken vooraf mee te delen aan de onderzoeksrechter, hetgeen een enorme administratieve werklast met zich meebrengt, is er geopteerd om in de toekomst per dossier een lijst van namen bij te laten houden, zodat er naderhand kan worden gecontroleerd wie wanneer de telefoontap afhandelde. Op deze manier zijn er adequatere gegevens beschikbaar, en kan er ook flexibeler worden gewerkt, terwijl er toch afdoende garanties zijn ingebouwd ter controle.

Si le taux de la peine indiqué au § 2 n’était pas adapté, une différence injustifiable subsisterait entre, d’une part, les opérateurs, les fournisseurs de services de communications électroniques, etc. et, d’autre part, d’autres personnes qui ne prêtent pas leur concours. En outre, la capacité financière de la première catégorie (personnes morales) est généralement bien supérieure à celle des personnes physiques.

§ 3.

Dans la pratique, il est impossible pour les officiers et agents de la police judiciaire de traiter toutes les écoutes téléphoniques (certainement en ce qui concerne l’écoute et la transcription dactylographique). C’est pourquoi ils doivent pouvoir recourir à des civils susceptibles d’effectuer ces tâches, en l’occurrence les membres du personnel CaLog. Il ne s’agit pas d’ouvrir cette possibilité à n’importe quel membre du personnel CaLog. Des conditions précises, notamment en termes de formation, seront prévues par le Roi.

Deux types de tâches ne peuvent en aucun cas être laissées aux membres du personnel du CaLog: l’analyse du contenu des communications ou données enregistrées et la sélection des parties pertinentes. Les membres du personnel du CaLog peuvent toutefois analyser le contenu de certains enregistrements s’il s’agit d’une expertise spécifique.

Exemple concret: en cas d’”écoutes IP”, il peut être nécessaire, du fait de la complexité des données techniques recueillies, de faire appel à du personnel technique bien formé du CaLog afin de procéder au classement et à la préanalyse de ces données...

Quelques tâches pouvant être confiées au personnel du CaLog:

— écoute et transcription d’écoutes téléphoniques;

— aide à la traduction;

— tâches administratives: archivage des données, etc.

Au lieu de communiquer préalablement au juge d’instruction le nom des personnes qui collaborent au dossier, ce qui entraîne une énorme charge de travail administrative, il a été décidé de faire conserver à l’avenir, par dossier, une liste de noms afin de pouvoir contrôler par la suite qui s’est chargé de l’écoute téléphonique et quand. Cela permet de disposer de données plus adéquates et de travailler de manière plus flexible tout en incluant quand même des garanties efficaces en matière de contrôle.

§ 4.

In deze paragraaf wordt aan de onderzoeksrechter de mogelijkheid verleend om personen waarvan de onderzoeksrechter vermoed dat ze een bijzondere kennis hebben van het communicatiemiddel of het informaticasysteem waarop de maatregel van toepassing is of van diensten of toepassingen om gegevens, die worden opgeslagen, verwerkt of overgedragen via een communicatiemiddel of een informaticasysteem, te beveiligen, te coderen of te versleutelen, rechtstreeks of via een politiedienst aangewezen door de Koning, te vorderen om inlichtingen te verlenen.

Wat betreft het toepassingsgebied van deze maatregel, kan verwezen worden naar de uitleg die is opgenomen bij artikel 88*quater*.

Er worden een aantal kleine wijzigingen doorgevoerd. Net als in de andere artikelen van dit ontwerp moet er zowel een verwijzing zijn naar een communicatiemiddel als naar een informaticasysteem.

Het "coderen" van gegevens houdt in dat deze worden omgezet naar een andere indeling of vorm. De term wordt ingevoegd omdat dit de tegenhanger is van het begrip "decoderen", dat opgenomen is in artikel 90*ter*, § 1, derde lid, derde streepje.

Er zal via een Koninklijk Besluit een politiedienst worden aangewezen die kan tussenkomen om de vordering van de onderzoeksrechter als bepaald in deze paragraaf uit te voeren.

Naar analogie van de wijzing in artikel 90*quater*, § 2, werd ook in deze paragraaf toegevoegd dat de onderzoeksrechter een beroep kan doen op een politiedienst aangewezen door de Koning. De wijziging van "Hij" naar "iedere persoon…" in het derde lid, is om duidelijker te stellen dat er strenger zal worden opgetreden tegen degenen die niet meewerken om de gevraagde gegevens te verkrijgen.

Zij die hun technische medewerking weigeren, kunnen gestraft worden met een geldboete 26 euro tot twintigduizend euro.

Bovendien is iedereen die uit hoofde van zijn bediening kennis krijgt van een maatregel of gevorderd wordt zijn technische medewerking te verlenen, verplicht tot geheimhouding.

§ 4.

Dans ce paragraphe, le juge d'instruction se voit conférer la possibilité d'exiger la fourniture d'informations de la part de personnes dont il présume qu'elles ont une connaissance particulière du moyen de communication ou du système informatique qui fait l'objet de la mesure ou de services ou applications qui permettent de protéger, de coder ou de crypter les données qui sont stockées, traitées ou transmises par un moyen de communication ou un système informatique, directement ou par l'intermédiaire d'un service de police désigné par le Roi, qu'elles fournissent des informations.

En ce qui concerne le champ d'application de cette mesure, il peut être renvoyé à l'explication donnée pour l'article 88*quater*.

Quelques petites modifications sont apportées. Comme dans les autres articles du présent projet, il convient d'évoquer tant un moyen de communication qu'un système informatique.

Le "cryptage" de données implique leur transposition dans une autre répartition ou sous une autre forme. Le terme est inséré parce qu'il est le pendant de la notion de "décryptage" figurant à l'article 90*ter*, § 1er, alinéa 3, troisième tiret.

Un service de police sera désigné par arrêté royal pour intervenir afin d'exécuter la réquisition du juge d'instruction telle que définie dans le présent paragraphe.

Par analogie avec la modification à l'article 90*quater*, § 2, il a également été ajouté dans le présent paragraphe que le juge d'instruction peut recourir à un service de police désigné par le Roi. Le remplacement, au troisième alinéa, du mot "Celui" par les mots "Toute personne" sert à indiquer de manière plus explicite que la sanction sera plus sévère à l'encontre de ceux qui ne prêtent pas leur concours à la fourniture des données demandées.

Ceux qui refusent de prêter leur concours technique peuvent être punis d'une amende de vingt-six euros à vingt mille euros.

En outre, toute personne qui, du chef de sa fonction, a connaissance d'une mesure ou est requise d'y prêter son concours technique, est tenue au secret.

Nieuwe § 5

Paragraaf 5 bepaalt dat, wanneer een zoeking in een informaticasysteem wordt bevolen, artikel 39*bis*, § 3, vierde lid toepasbaar is.

Artikel 19

Aangezien artikel 90*quater* van het Wetboek van strafvordering werd aangepast in verband met de machtiging, moet ook artikel 90*quinquies* worden aangepast.

Er wordt aan het einde van het eerste lid een verduidelijking gegeven betreffende de termijn van zes maanden. Deze termijn van zes maanden vangt aan de dag van de eerste machtiging waarbij de maatregel wordt bevolen, en loopt tot en met de dag voor de zoveelste van de zesde daarop volgende maand.

Indien de maatregel echter pas na de dag van de eerste machtiging daadwerkelijk kon aanvangen, omdat de technische voorbereiding van de maatregel enige tijd in beslag nam, begint de termijn van zes maanden te lopen op de dag waarop de maatregel daadwerkelijk werd aangevat, dat wil zeggen op de dag waarop de bewijsgaring begon.

Op grond van deze bepaling wordt dus, voor de berekening van de maximumtermijn van zes maanden, geen rekening gehouden met de tijd die de politiediensten nodig hadden om de technische voorbereiding van de maatregel van artikel 90*ter* mogelijk te maken.

Deze bepaling werd uitgewerkt om te remediëren aan een onwenselijke toestand. Vandaag worden onderzoeksrechters namelijk vaak geconfronteerd met situaties waarbij de technische voorbereiding van een maatregel tot direct afluisteren op zich al een aantal weken in beslag neemt, zodat in totaal minder dan zes maanden effectief afgeluisterd kan worden. De zesmaandentermijn begint in het huidige recht immers te lopen vanaf de dag van de eerste machtiging, ongeacht of de maatregel die dag ook effectief werd aangevat.

Deze vaststelling strookt niet met het doel van de zesmaandentermijn. Deze beoogt de privacy van betrokkenen te waarborgen door afluistermaatregelen van langer dan zes maanden te verbieden. Zolang de maatregel nog in een technische voorbereidingsfase zit, wordt de privacy echter slechts miniem aangetast, zodat het gerechtvaardigd is geen rekening te houden met deze periode voor de berekening van de maximumtermijn van zes maanden.

Nouveau § 5

Le paragraphe 5 prévoit que si une recherche dans un système informatique est ordonnée, l'article 39*bis*, § 3, alinéa 4, est d'application.

Article 19

Étant donné que l'article 90*quater* du Code d'instruction criminelle a été adapté au niveau de l'autorisation, l'article 90*quinquies* doit lui aussi être adapté.

Une précision relative au délai de six mois est donnée à la fin de l'alinéa 1er. Ce délai de six mois commence à courir le jour de la première autorisation ordonnant la mesure et s'achève la veille du quantième du sixième mois suivant.

Toutefois, si la mesure n'a pu débuter effectivement qu'après le jour de la première autorisation, parce que la préparation technique de la mesure a pris un certain temps, le délai de six mois commence à courir le jour où la mesure a effectivement débuté, à savoir le jour où la collecte des preuves a commencé.

Sur la base de cette disposition, il n'est donc pas tenu compte pour le calcul du délai maximum de six mois, du temps nécessaire aux services de police pour permettre la préparation de la mesure de l'article 90*ter*.

Cette disposition a été élaborée afin de remédier à une situation non souhaitable. En effet, aujourd'hui les juges d'instruction sont souvent confrontés à des situations où la préparation technique d'une mesure d'écoute directe nécessite en soi plusieurs semaines, de sorte que l'écoute en elle-même s'effectue au total sur moins de six mois. Dans le droit actuel, le délai de six mois commence en effet à courir le jour de la première autorisation, quel que soit le jour où la mesure débute effectivement.

Ce constat est contradictoire par rapport à la finalité du délai de six mois. Celle-ci a pour but de préserver la vie privée des personnes concernées en interdisant les mesures d'écoute de plus de six mois. Toutefois, tant que la mesure est encore dans une phase technique de préparation, l'atteinte à la vie privée est minime. Il est dès lors légitime de ne pas tenir compte de cette période pour calculer le délai de six mois maximum.

Voortaan zullen politiediensten maximum twee maanden extra tijd krijgen om de voorbereidende handelingen te treffen die de tenuitvoerlegging van de maatregel van artikel 90*ter*, § 1, mogelijk maken.

Het feit dat de zesmaandentermijn later kan aanvangen dan de dag van de eerste machtiging, heeft niet tot gevolg dat de politiediensten technische voorbereidingshandelingen kunnen stellen zonder machtiging van een onderzoeksrechter.

Indien de eerste machtiging voor een termijn van een maand werd verleend, en de politiediensten merken dat de technische voorbereiding langer zal duren dan een maand, dient de onderzoeksrechter tijdig te worden gecontacteerd voor een eventuele verlenging.

Dit heeft tot gevolg dat de onderzoeksrechter maximum acht opeenvolgende machtigingen van een maand kan verlenen voor eenzelfde maatregel (maximum twee voor technische voorbereiding en maximum zes voor effectieve uitvoering van de maatregel).

Concreet voorbeeld:

De onderzoeksrechter machtigt een heimelijke zoeking in een informaticasysteem op 15 september, geldig voor een maand. Op 15 oktober staat hij een verlenging met een maand toe, aangezien de technische hulpmiddelen nog niet konden worden aangebracht. Pas op 30 oktober zijn die hulpmiddelen geplaatst en gaat de heimelijke zoeking effectief van start. Op deze dag begint de termijn van zes maanden te lopen.

Artikel 20

Artikel 20 vervangt artikel 90*sexies* van het Wetboek van strafvordering.

Paragraaf 1 van artikel 90*sexies* Sv. geeft mee wat de officieren van gerechtelijke politie dienen ter beschikking te stellen aan de onderzoeksrechter. Dit wetsontwerp verruimt en verduidelijkt bovenvermelde zaken.

Zo gaat het om bestanden die opgenomen niet voor het publiek toegankelijke communicaties bevatten of om gegevens bekomen van een informaticasysteem (1°). Deze bepaling is aangepast aan de veranderde terminologie in artikel 90*ter*, § 1 Sv.

Ook de overschrijving of weergave van de door de aangewezen officieren van gerechtelijke politie voor het onderzoek van belang geachte gedeelten van de

Désormais, les services de police disposeront au maximum de deux mois supplémentaires pour prendre les actions préparatoires permettant d'exécuter la mesure de l'article 90*ter*, § 1er.

Le fait que le délai de six mois puisse débuter plus tard que le jour de la première autorisation n'implique pas que les services de police pourront poser des actes techniques préparatoires sans l'autorisation d'un juge d'instruction.

Si la première autorisation a été accordée pour un délai d'un mois et que les services de police remarquent que la préparation technique durera plus d'un mois, le juge d'instruction doit être contacté à temps en vue d'une prolongation éventuelle.

Il en résulte que le juge d'instruction peut accorder au maximum huit autorisations consécutives d'un mois pour une même mesure (maximum deux pour la préparation technique et maximum six pour l'exécution effective de la mesure).

Exemple concret:

Le juge d'instruction autorise une recherche en secret dans un système informatique le 15 septembre, valable un mois. Le 15 octobre, il autorise une prolongation d'un mois étant donné que les moyens techniques n'ont pas encore pu être mis en place. Ces moyens ne sont installés que le 30 octobre et la recherche en secret débute effectivement. Le délai de six mois commence à courir à cette date.

Article 20

L'article 20 remplace l'article 90*sexies* du Code d'instruction criminelle.

Le paragraphe 1er de l'article 90*sexies* du Code d'instruction criminelle indique ce que les officiers de la police judiciaire doivent mettre à la disposition du juge d'instruction. Le présent projet de loi étend et précise les éléments précités.

Tel est le cas de fichiers contenant des communications non accessibles au public qui ont été enregistrées ou de données provenant d'un système informatique (1°). Cette disposition a été adaptée à la terminologie modifiée à l'article 90*ter*, § 1er, du Code d'instruction criminelle.

De même, la transcription ou reproduction des parties des communications ou données enregistrées estimées pertinentes pour l'instruction par les officiers de police

opgenomen communicaties of gegevens (2°) moet ter beschikking van de onderzoeksrechter worden gesteld.

De term “weergave” wordt gehanteerd voor gegevens van informaticasystemen die door hun aard niet kunnen overgeschreven worden, zoals foto’s.

Een nieuw punt 3° wordt geïntroduceerd in § 1 dat luidt: “in voorkomend geval, de plaats van de gegevens, bedoeld in 2°, in het informaticasysteem.”

Met “in voorkomend geval” wordt bedoeld “indien er een plaats kan worden aangewezen”. Voorbeeld hierbij is de bestandslocatie op computersystemen, zoals bv. “C://Gebruikers/Naam/Afbeeldingen/Plantage 1/…”.

Het vermelden van deze informatie moet toelaten dat een en ander in zijn context kan worden geplaatst.

Tenslotte stellen de officieren van gerechtelijke politie ter beschikking: een algemene beschrijving van de inhoud en van de identificatiegegevens van de gebruikte communicatiemiddelen of informaticasystemen wat betreft de niet van belang geachte communicaties of gegevens (4°).

Op basis van deze algemene beschrijving moet het mogelijk zijn snel een idee te krijgen over de (globale) inhoud van de niet relevant geachte communicaties of gegevens. Het is evenwel niet de bedoeling dat elke communicatie of elk bestand een label krijgt.

Artikel 90*sexies* voorziet in zijn § 3 dat verzamelde gegevens die onder het beroepsgeheim vallen, niet worden opgetekend in het proces-verbaal. Wanneer toch elementen gedekt door het beroepsgeheim opgenomen zijn in het dossier, zullen deze door de feitenrechter uit het debat geweerd worden.

Artikel 21

Artikel 21 herschrijft artikel 90*septies* van het Wetboek van strafvordering om het beter leesbaar te maken. Er zijn ook een aantal aanpassingen gebeurd die er voor zorgen dat het gemakkelijker wordt om de opnames achteraf te controleren (zie § 2).

In paragraaf 3 worden drie uitzonderingen voorzien op de verplichte vernietiging door de politiediensten van iedere aantekening in het kader van de tenuitvoerlegging van de maatregelen van artikelen 90*ter*, 90*quater* en 90*quinquies*. De Raad van State stelt de vraag of er niet moet voorzien worden in een specifieke termijn voor deze vernietiging. De regering merkt op dat dit in

judiciaire commis (2°) doit être mise à la disposition du juge d’instruction.

Le terme “reproduction” est utilisé pour des données provenant de systèmes informatiques et qui par leur nature ne peuvent être transcrites, comme notamment les photos.

Au § 1er, il est inséré un nouveau point 3° rédigé comme suit: “le cas échéant, l’endroit où se trouvent les données visées au 2° dans le système informatique.”

Par “le cas échéant”, il y a lieu d’entendre “si une place peut être désignée”. Par exemple, l’emplacement des fichiers dans les systèmes informatiques (p. ex. “C:// Utilisateurs/Nom/Images/Plantation 1/…”).

La mention de cette information doit permettre une mise en contexte.

Enfin, les officiers de la police judiciaire mettent à disposition: une description générale du contenu et des données d’identification des moyens de communication ou systèmes informatiques utilisés en ce qui concerne les communications ou données estimées non pertinentes (4°).

Cette description générale doit permettre de se faire rapidement une idée du contenu (global) des communications ou données considérées comme non pertinentes. Le but n’est toutefois pas d’étiqueter chaque communication ou chaque fichier.

L’article 90*sexies* prévoit en son § 3 que les données qui sont couvertes par le secret professionnel ne sont pas consignées dans le procès-verbal. Si toutefois des données couvertes par le secret professionnel figurent dans le dossier, elles devront être écartées des débats par le juge du fond.

Article 21

L’article 21 réécrit l’article 90*septies* du Code d’instruction criminelle afin de le rendre plus lisible. Un certain nombre d’adaptations ont également été apportées afin de faciliter le contrôle ultérieur des enregistrements (voir § 2).

Au paragraphe 3, trois exceptions sont prévues à la destruction obligatoire par les services de police de toute note prise dans le cadre de l’exécution des mesures visées aux articles 90*ter*, 90*quater* et 90*quinquies*. Le Conseil d’État pose la question de savoir si un délai spécifique ne doit pas être prévu pour cette destruction. Le gouvernement observe que la version actuelle

de huidige versie van artikel 90*septies* evenmin is bepaald en vindt het bovendien niet opportuun een precies tijdstip te bepalen. In de praktijk gebeurt de vernietiging steeds ten laatste wanneer de zaak definitief is beslecht doordat het vonnis of arrest in kracht van gewijsde is getreden.

Ten eerste moeten de aantekeningen die verband houden met het bepaalde in artikel 90*sexies*, § 1, 2°, 3° en 4° niet vernietigd worden.

Ten tweede mogen de gegevens worden bewaard die stemherkenning mogelijk maken, zoals bedoeld in artikel 33 van dit voorontwerp van wet.

Ten derde mogen de strikt noodzakelijke administratieve gegevens bewaard blijven bij de dienst aangewezen door de Koning. Dit mag enkel om beheersredenen en om aan de verplichting van artikel 90*decies* (verslag aan het Parlement) te kunnen voldoen. Met "beheersredenen" worden doeleinden bedoeld zoals het bijhouden van statistieken, het kunnen uitvoeren van interne of externe (kwaliteits-, veiligheids-,…)controles, en dergelijke meer.

Administratieve gegevens zijn bijvoorbeeld het type telefoonnummer, de namen van de vertalers die toegang hadden tot een bepaald dossier tijdens een bepaald periode, de naam van de magistraat die de machtiging verleende, een lijst met storingen of defecten die plaatshadden tijdens de uitvoering van een bepaalde maatregel, het type criminaliteit waarvoor de maatregel werd bevolen, etc. Het mag niet gaan om gegevens uit de processen-verbaal, om de geregistreerde communicatie of gegevens zelf, of om gegevens waaruit de identiteit blijkt van de verdachten die het voorwerp van de maatregel hebben uitgemaakt.

Paragraaf 4 werd gewijzigd opdat de opgenomen communicaties of gegevens van een informaticasysteem, bedoeld in artikel 90*sexies*, § 1, 1°, ook kunnen bewaard blijven bij de dienst aangewezen door de Koning. Het gaat om een aanvullende kopie, bovenop deze die ter griffie wordt bewaard.

Het doel van deze bepaling is ervoor te zorgen dat de opnames niet verloren gaan, bijvoorbeeld door een slechte bewaring ter griffie of doordat een verdachte deze vernietigd heeft bij het bekijken of beluisteren ervan. De dienst aangewezen door de Koning moet voldoende garanties bieden dat de opnames op zo'n manier worden bewaard dat ze voor lange tijd intact blijven én dat geen onbevoegde personen er toegang toe krijgen. De noodzakelijke garanties zullen vastgesteld worden door de Koning.

de l'article 90*septies* n'en détermine pas non plus et estime en outre qu'il n'est pas opportun de déterminer un moment précis. Dans la pratique, la destruction a toujours lieu au plus tard lorsque l'affaire est définitivement tranchée en raison du fait que le jugement ou l'arrêt est passé en force de chose jugée.

Premièrement, les notes qui ont un rapport avec le prescrit de l'article 90*sexies*, § 1er, 2°, 3° et 4°, ne doivent pas être détruites.

Deuxièmement, les données permettant la reconnaissance vocale, telle que visée à l'article 33 du présent projet de loi.

Troisièmement, les données administratives strictement nécessaires peuvent être conservées au sein du service désigné par le Roi. Cela n'est autorisé que pour des raisons de gestion et en vue du respect de l'obligation de l'article 90*decies* (rapport au Parlement). Par "raisons de gestion" on entend des objectifs comme, entre autres, la tenue de statistiques et la capacité d'effectuer des contrôles (de qualité, de sécurité, etc.) internes ou externes.

Des données administratives sont, par exemple, le type de numéro de téléphone, les noms des traducteurs ayant eu accès à un dossier déterminé pendant une période déterminée, le nom du magistrat qui avait accordé l'autorisation, une liste des dérangements ou pannes qui s'étaient produits durant l'exécution d'une mesure déterminée, le type de criminalité pour laquelle la mesure avait été ordonnée, etc. Il ne peut pas s'agir de données issues des procès-verbaux, de la communication enregistrée ou des données enregistrées mêmes, ou de données dont ressort l'identité des suspects qui ont fait l'objet de la mesure.

Le paragraphe 4 a été modifié afin que les communications ou données enregistrées d'un système informatique visées à l'article 90*sexies*, § 1er, 1°, puissent également être conservées au sein du service désigné par le Roi. Il s'agit d'une copie additionnelle à celle conservée au greffe.

L'objectif de cette disposition est de veiller à ce que les enregistrements ne se perdent pas en raison notamment d'une mauvaise conservation au greffe ou d'une destruction par un suspect au moment où il visionne ou écoute l'enregistrement. Le service désigné par le Roi doit offrir suffisamment de garanties du fait que les enregistrements sont conservés de manière à demeurer intacts durant une longue période et qu'aucune personne non habilitée ne peut y avoir accès. Les garanties nécessaires seront définies par le Roi.

De wijzigingen in paragraaf 6 beogen het recht van de verdediging te waarborgen aangaande de overschrijving van de opnames. Het moet immers steeds mogelijk zijn voor de verdediging om de volledige communicaties of gegevens van een informaticasysteem waaruit bepaalde gedeelten van belang werden geacht voor het onderzoek en dus werden overgeschreven of weergegeven, te raadplegen.

Gedeelten van communicaties of gegevens dienen immers beoordeeld te kunnen worden in het kader van de context ervan. De partijen moeten over de mogelijkheid beschikken om deze communicaties of gegevens te raadplegen en eventueel een bijkomende overschrijving of weergave te vragen.

De partijen dienen daartoe een verzoek te richten tot de rechter. Indien het verzoek gericht wordt tot de onderzoeksrechter, wordt dit behandeld overeenkomstig artikel 61*quinquies* van het Wetboek van Strafvordering.

De rechter kan het verzoek afwijzen om drie redenen:

— Indien hij de inwilliging van het verzoek niet noodzakelijk acht om de waarheid aan de dag te brengen;

— Indien hij de inwilliging van het verzoek op dat moment nadelig acht voor het onderzoek; of

— Om redenen die verband houden met de bescherming van andere rechten of belangen van personen.

De eerste twee weigeringsgronden werden overgenomen uit artikel 61*quinquies*, § 3 Sv.

De rechter kan, op grond van voornoemde redenen, van oordeel zijn dat een weigering van het verzoek niet opportuun is, maar dat het gevraagde toch in zekere zin beperkt moet worden. In dat geval kan hij het verzoek in beperkte mate toestaan, waarbij hij duidelijk aangeeft welke bestanden of stukken mogen geraadpleegd worden of bijkomend overgeschreven of weergegeven moeten worden.

Artikel 22

Dit artikel betreft artikel 90*octies* van het Wetboek van strafvordering, meer bepaald de mogelijkheid om de zoeking in een informaticasysteem toe te passen op advocaten en artsen. De uitzondering voor advocaten en artsen werd ingegeven door de overweging dat deze beroepscategorieën bij uitstek het gevaar lopen om te worden geconfronteerd met verdachten, waarmee zij door hun beroepssituatie in een vertrouwelijke relatie

Les modifications apportées au paragraphe 6 visent à garantir le droit de la défense concernant la transcription des enregistrements. En effet, la défense doit toujours avoir la possibilité de consulter la totalité des communications ou données d'un système informatique dont certains passages ont été estimés pertinents pour l'enquête et donc transcrits ou reproduits.

Il faut effectivement pouvoir évaluer des passages de communications ou de données dans le cadre de leur contexte. Les parties doivent avoir la possibilité de consulter ces communications ou données et, éventuellement, d'en demander une transcription ou une reproduction additionnelle.

Les parties doivent adresser une demande au juge à cet effet. Si la demande est adressée au juge d'instruction, elle est examinée conformément à l'article 61*quinquies* du Code d'instruction criminelle.

Le juge peut rejeter la demande pour trois raisons:

— lorsqu'il considère que l'acceptation de la demande n'est pas nécessaire à la manifestation de la vérité;

— lorsqu'il considère que l'acceptation de la demande est, à ce moment, préjudiciable à l'instruction; ou

— pour des raisons liées à la protection d'autres droits ou intérêts de personnes.

Les deux premiers motifs de refus proviennent de l'article 61*quinquies*, § 3, du Code d'instruction criminelle.

Sur la base des raisons précitées, le juge peut estimer inopportun un rejet de la demande, mais que la demande doit être limitée d'une certaine manière. Dans ce cas, il peut accéder à la demande de manière limitée en indiquant clairement quels fichiers ou pièces peuvent être consultés ou doivent faire l'objet d'une transcription ou d'une reproduction additionnelle.

Article 22

Cet article concerne l'article 90*octies* du Code d'instruction criminelle, plus précisément la possibilité d'appliquer la recherche dans un système informatique aux avocats et aux médecins. L'exception pour les avocats et les médecins était dictée par la considération que ces catégories professionnelles sont par excellence exposées au risque d'être confrontées à des suspects avec qui, en raison de leur situation professionnelle,

verkeren die in het bijzonder beschermd moet worden. Dit is de klassieke beschermingsclausule zoals die ook voorkomt in gelijkaardige onderzoeksmaatregelen, zoals het inkijken van post (art. 88*sexies* van het Wetboek van strafvordering), een observatie met zicht in een woning (art. 56*bis* van het Wetboek van strafvordering) of een inkijkoperatie (art. 89*ter* van het Wetboek van strafvordering). Deze bescherming is al bekend en heeft dus geen verdere uitleg nodig.

Ook wordt een geheimhoudingsplicht ingeschreven voor de stafhouder en de vertegenwoordiger van de provinciale orde van geneesheren, wanneer zij op de hoogte worden gebracht van een maatregel.

Net zoals bij deze andere onderzoeksmaatregelen wordt hier niet voorzien in een specifieke bescherming voor journalisten. De bescherming van het bronnengeheim van journalisten wordt immers gegarandeerd door artikel 5 van de wet van 7 april 2005 tot bescherming van de journalistieke bronnen: “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 de in artikel 4 bedoelde misdrijven worden gepleegd, en met naleving van de daarin bepaalde voorwaarden.” De wet van 7 april 2005 is een bijzondere wet, die toepasselijk is ongeacht de specifieke situatie waarin de beschermde persoon zich bevindt.

Paragraaf 3, laatste lid betreft specifiek de gegevens die onder het beroepsgeheim vallen. Ter bescherming van dit beroepsgeheim worden de gegevens afzonderlijk ter griffie bewaard. Op die manier kan achteraf in voorkomend geval nog toepassing worden gemaakt van artikel 90*septies*, § 6, tweede lid Sv. (m.b.t. het verzoek tot raadpleging of bijkomende overschrijving van de “andere bestanden of gegevens”).

Artikel 23

Dit artikel bepaalt dat de persoon ten aanzien van wie de maatregel van de heimelijke zoeking in een informaticasysteem is genomen, schriftelijk in kennis gesteld moet worden van de aard van die maatregel en van de dagen waarop deze is uitgevoerd, tenzij diens identiteit of woonplaats redelijkerwijze niet achterhaald kan worden.

elles entretiennent une relation de confiance qui doit tout particulièrement être préservée. Il s’agit de la clause de protection classique telle qu’elle apparaît également dans des mesures d’investigation similaires comme l’ouverture de courrier (article 88*sexies* du Code d’instruction criminelle), une observation afin d’avoir une vue dans un domicile (article 56*bis* du Code d’instruction criminelle) ou un contrôle visuel discret (article 89*ter* du Code d’Instruction criminelle). Cette protection est déjà connue et ne nécessite donc pas d’autre commentaire.

Il est également prévu une obligation de secret pour le bâtonnier et le représentant de l’ordre provincial des médecins lorsqu’ils sont avertis d’une mesure.

Tout comme c’est le cas pour ces autres mesures d’instruction, aucune protection spécifique n’est prévue pour les journalistes. La protection du secret des sources journalistiques est en effet garantie par l’article 5 de la loi du 7 avril 2005 relative à la protection des sources journalistes: “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 des infractions visées à l’article 4, et dans le respect des conditions qui y sont définies.”. La loi du 7 avril 2005 est une loi spéciale, applicable quelle que soit la situation dans laquelle se trouve la personne protégée.

Le paragraphe 3, dernier alinéa, concerne spécifiquement les données couvertes par le secret professionnel. En vue de la protection de ce secret professionnel, les données sont conservées séparément au greffe. De cette manière, il est encore possible par la suite, le cas échéant, d’appliquer l’article 90*septies*, § 6, alinéa 2, CIC (en ce qui concerne la requête de consultation ou de copies supplémentaires des “autres fichiers ou données”).

Article 23

Cet article prévoit que la personne faisant l’objet de la mesure de recherche en secret dans un système informatique doit être informée par écrit de la nature de cette mesure et des dates auxquelles elle a été exécutée, sauf si son identité ou son adresse ne peut être raisonnablement retrouvée.

Artikel 24

De maatregel bedoeld in artikel 46*quinquies* van het Wetboek van strafvordering (interactie/infiltratie op internet) wordt toegevoegd aan de lijst van artikelen in artikel 90*decies* waarover de minister van Justitie een jaarlijks rapport moet voorleggen aan het Parlement.

Artikel 25

De controle van de kamer van inbeschuldigingstelling op de bijzondere opsporingsmethoden, observatie en infiltratie wordt uitgebreid naar de maatregel voorzien in het nieuwe artikel 46*sexies* van het Wetboek van strafvordering (interactie/infiltratie op internet).

Met de zinsnede "indien daarbij een vertrouwelijk dossier werd aangelegd" wordt gedoeld op het feit dat de toepassing van de maatregel van artikel 46*sexies* van het Wetboek van strafvordering niet steeds aanleiding zal geven tot de creatie van een vertrouwelijk dossier. Enkel als de procureur des Konings misdrijven machtigt of een burgerdeskundige inschakelt, moet hij een vertrouwelijk dossier aanleggen. (Zie *supra* de toelichting bij artikel 46*sexies*.)

Artikel 26

Ook het feit dat de kamer van inbeschuldigingstelling voorlopig, ambtshalve, op verzoek van de onderzoeksrechter of op vordering van het openbaar ministerie, tijdens het gerechtelijk onderzoek, de regelmatigheid van de bijzondere opsporingsmethoden, observatie en infiltratie kan onderzoeken, wordt uitgebreid met het nieuwe 46*sexies* Sv. (interactie/infiltratie op internet).

Artikel 27

Artikel 464/13 wordt in dezelfde zin gewijzigd als artikel 46*bis* (zie de uitgebreide toelichting bij dit artikel). De term "verstrekker van een elektronische communicatiedienst" wordt vervangen door een nieuwe, ruimere omschrijving die overeenstemt met de interpretatie van het Hof van Cassatie in zijn "Yahoo-arrest" van 18/01/2011. Daarnaast wordt de termijn voor het verlenen van medewerking aangepast naar "in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering".

Article 24

La mesure visée à l'article 46*quinquies* du Code d'instruction criminelle (interaction/infiltration sur l'Internet) est ajoutée à la liste des articles sur lesquels le ministre de la Justice doit faire rapport annuellement au Parlement.

Article 25

Le contrôle exercé par la chambre des mises en accusation sur les méthodes particulières de recherche, d'observation et d'infiltration est étendu aux mesures prévues au nouvel article 46*sexies* du Code d'instruction criminelle (interaction/infiltration sur Internet).

Le membre de phrase "si un dossier confidentiel a été ouvert dans ce cadre" vise le fait que l'application de la mesure de l'article 46*sexies* du Code d'instruction criminelle ne donnera pas toujours lieu à la création d'un dossier confidentiel. Ce n'est que si le procureur du Roi autorise des infractions ou fait appel à un expert civil qu'il devra constituer un dossier confidentiel. (Voir *supra* le commentaire de l'article 46*sexies*).

Article 26

Le nouvel article 46*sexies* du Code d'instruction criminelle étend également a possibilité pour la chambre des mises en accusation d'examiner, à titre provisoire, d'office, à la demande du juge d'instruction ou à la requête du ministère public, durant l'instruction, la régularité des méthodes particulières de recherche, et d'instruction (interaction/infiltration sur Internet).

Article 27

L'article 464/13 est modifié dans le même sens comme l'article 46*bis* (voir commentaire détaillé de cet article). Les termes "fournisseur d'un service de communications électroniques" sont remplacés par une nouvelle définition, plus large, conforme à l'interprétation de la Cour de cassation dans son "arrêt Yahoo" du 18/01/2011. En outre, le délai pour prêter sa collaboration est adapté et devient "en temps réel ou, le cas échéant, au moment précisé dans la réquisition".

Artikel 28

Artikel 464/25 wordt in dezelfde zin gewijzigd als artikel 46*bis* (zie de uitgebreide toelichting bij dit artikel). De term “verstrekker van een elektronische communicatiedienst” wordt vervangen door een nieuwe, ruimere omschrijving die overeenstemt met de interpretatie van het Hof van Cassatie in zijn “Yahoo-arrest” van 18/01/2011. Daarnaast wordt de termijn voor het verlenen van medewerking aangepast naar “in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering”.

TITEL 3

Bepalingen tot wijziging van het Strafwetboek

Artikelen 29, 30, 31 en 32

Deze artikelen wijzigen de artikelen 259*bis* en 314*bis* van het Strafwetboek en hun opschriften, en zijn terminologisch van aard.

Immers, door de wijzigingen aangebracht aan de artikelen 90*ter* en volgende van het Wetboek van strafvordering, dient dezelfde terminologie gebruikt te worden in de artikelen die het geheim van de privécommunicatie en -telecommunicatie beschermen. Daarom wordt ook hier de term “niet voor publiek toegankelijke communicatie” ingevoerd en wordt de voorwaarde “tijdens de overbrenging ervan” geschrapt.

De strafbaarstellingen in deze artikelen zijn evenwel niet uitgebreid tot “gegevens van een informaticasysteem”, aangezien dit reeds bestraft wordt als het misdrijf “hacking” (artikel 550*bis* Strafwetboek).

Artikel 33

De oprichting van een gegevensbank van stemafdrukken strekt ertoe met behulp van software de stem te herkennen van verdachten en veroordeelde personen van wie de stemafdruk reeds geregistreerd is in het kader van dossiers waarvoor een telefoontap (thans of in het verleden) is goedgekeurd door de bevoegde magistraat.

Dit hulpmiddel voor de identificatie aan de hand van de stemafdruk kan een hulp zijn bij het afluisteren in het kader van eenzelfde gerechtelijk dossier en bij het leggen van verbanden tussen verschillende gerechtelijke dossiers.

Article 28

L’article 464/25 est modifié dans le même sens comme l’article 46*bis* (voir commentaire détaillé de cet article). Les termes “fournisseur d’un service de communications électroniques” sont remplacés par une nouvelle définition, plus large, conforme à l’interprétation de la Cour de cassation dans son “arrêt Yahoo” du 18/01/2011. En outre, le délai pour prêter sa collaboration est adapté et devient “en temps réel ou, le cas échéant, au moment précisé dans la réquisition”.

TITRE 3

Dispositions modifiant le Code pénal

Articles 29, 30, 31 et 32

Ces articles modifient les articles 259*bis* et 314*bis* du Code pénal et leurs intitulés, et sont d’ordre terminologie.

En effet, compte tenu des modifications apportées aux articles 90*ter* et suivants du Code d’instruction criminelle, la même terminologie doit être utilisée aux articles qui protègent le secret des communications et télécommunications privées. Pour cette raison, les termes “communications non accessibles au public” sont insérés et l’exigence “durant leur transmission” est supprimée.

Dans ces articles, les incriminations ne sont toutefois pas étendues aux “données d’un système informatique” puisque cette infraction est déjà punissable en tant que “hacking” (article 550*bis* du Code pénal).

Article 33

La création d’une banque de données des empreintes vocales a pour finalité d’aider à identifier, via un logiciel, sur la base de leurs voix, des suspects et des personnes condamnées, dont l’empreinte vocale a déjà été enregistrée dans le cadre de dossiers pour lesquels une écoute téléphonique est ou a été approuvée par le magistrat compétent.

Cette aide à l’identification via l’empreinte vocale permettra de réaliser une aide à l’écoute dans le cadre d’un même dossier judiciaire et, d’autre part, de réaliser des liens entre plusieurs dossiers judicaires.

Het gaat om een stemafdruk aangezien er op basis van de specifieke kenmerken van de stem een model met een unieke code zal worden gemaakt (naar analogie met de werkwijze die reeds wordt gebruikt voor de dactyloscopische afdrukken). Voor de doeltreffendheid van de software is het niet noodzakelijk om de stemstalen (opnames waarop de stem te horen is) te bewaren. Deze vallen dan ook niet onder de term "technische gegevens" in artikel 33 van dit wetsontwerp. Net zoals bij vingerafdrukken moet alleen de code die uit de omzettingsalgoritmen resulteert, worden bewaard in de gegevensbank.

Voorts kunnen enkel de stemafdrukken bewaard worden van personen die het voorwerp uitmaken of hebben uitgemaakt van een tapmaatregel en die bedoeld worden in artikel 44/5, § 3, 1° van de wet op het politieambt (verdachten en veroordeelde personen). Stemafdrukken van andere personen wiens stem opgenomen is bij een telefoontap, zoals getuigen of geheel toevallige betrokkenen, mogen niet worden aangemaakt of bewaard.

Het werken met een gegevensbank van stemafdrukken, gecombineerd met stemherkenningssoftware, levert tactische informatie op voor de politieambtenaren die belast zijn met de uitvoering van een telefoontap. De methode voor verwerking en vergelijking is niet voldoende onwankelbaar om als bewijs in rechte te kunnen worden gebruikt, noch à charge, noch à décharge.

Enkel politieambtenaren en leden van de organen die toezicht houden op de werking van de politiediensten (zoals het Vast Comité P) kunnen rechtstreeks of onrechtstreeks toegang krijgen tot de gegevensbank. Derden krijgen slechts toegang indien dit strikt noodzakelijk is voor de goede werking van de gegevensbank of de eraan gelinkte software.

Hulp bij het afluisteren – in het kader van eenzelfde gerechtelijk dossier

In deze situatie krijgen de officier van gerechtelijke politie en de agenten van gerechtelijke politie die belast zijn met de implementatie van een telefoontap zeer vaak te maken met moeilijkheden inzake het tactisch begrip van de informatie die is ingewonnen door de interceptie van communicatie, inzonderheid omdat het moeilijk is om de spreker te identificeren/herkennen.

De term "identificatie" moet hier niet worden begrepen als de formele vaststelling van de identiteit van de spreker, maar als de detectie dat een bepaalde persoon reeds heeft deelgenomen aan een geïntercepteerd gesprek in het dossier.

Il s'agit d'une empreinte vocale dans la mesure où la voix va, sur la base de ses caractéristiques propres, être modélisée en un code unique (tout comme il est actuellement procédé pour les empreintes dactyloscopiques). Pour que le logiciel soit efficace, il n'est pas nécessaire de garder les échantillons de voix (enregistrements sur lesquels on entend la voix). Ceux-ci ne tombent dès lors pas sous les termes "données techniques" dans l'article 33 du présent projet de loi. À l'instar de ce qui se fait pour les empreintes digitales, seul le code issu des algorithmes de conversion doit être sauvegardé dans la banque de données.

Désormais, seules pourront être conservées les empreintes vocales de personnes qui font ou ont fait l'objet d'une mesure d'écoute et qui sont visées à l'article 44/5, § 3, 1°, de la loi sur la fonction de police (suspects et personnes condamnées). Les empreintes vocales d'autres personnes dont la voix est enregistrée lors d'une écoute téléphonique, comme les témoins ou des personnes impliquées tout à fait par hasard, ne peuvent pas être établies ou conservées.

Le recours à une banque de données d'empreintes vocales, combiné à un logiciel de reconnaissance vocale, fournit des informations tactiques aux services de police chargés de l'exécution d'une mesure d'écoute téléphonique. La méthode de traitement et de comparaison n'est pas suffisamment indéfectible pour pouvoir être utilisée en justice, que ce soit à charge ou à décharge.

Seuls des fonctionnaires de police et des membres des organes qui contrôlent le fonctionnement des services de police (comme le Comité permanent P) peuvent avoir directement ou indirectement accès à la banque de données. Les tiers n'y ont accès que si cela s'avère strictement nécessaire au bon fonctionnement de la banque de données ou au logiciel qui y est associé.

Aide à l'écoute – dans le cadre d'un même dossier judiciaire

Dans cette situation l'officier de police judiciaire et les agents de police judiciaire chargés de la mise en œuvre d'une écoute téléphonique sont très régulièrement confrontés à des difficultés de compréhension tactique des informations récoltées par l'interception de communication, notamment suite à la complexité d'identifier/reconnaitre la personne qui parle.

Il faut entendre ici le terme identification non pas comme étant l'établissement formel de l'identité de celui qui parle mais bien détecter qu'une personne déterminée est déjà apparue dans une conversation interceptée dans le dossier.

Die moeilijkheden kunnen als volgt worden geïllustreerd:

— Wanneer in het kader van eenzelfde gerechtelijk dossier een of meer afgeluisterde apparaten worden gebruikt door een groot aantal personen (soms meer dan tien);

— Wanneer de daders in datzelfde kader geregeld van prepaid kaart wisselen (of onderling prepaidkaarten uitwisselen). Zo wordt een prepaid kaart in het kader van thans lopende gerechtelijke dossiers inzake mensenhandel gemiddeld 48 uur gebruikt.

Bovendien is het niet uitzonderlijk dat in dit soort dossiers tientallen nummers achtereenvolgens worden afgeluisterd.

Die moeilijke "identificatie" wordt nog ingewikkelder wanneer de afgeluisterde personen een vreemde taal (of zelfs meerdere vreemde talen) spreken.

In dat geval gebeurt een eventuele stemherkenning *de facto* door de aangewezen vertaler.

Indien de vertalingen door verschillende vertalers worden gemaakt, wordt die herkenning nog onzekerder.

Met stemherkenningssoftware kan een met een interceptiemaatregel belaste officier van gerechtelijke politie gemakkelijk bepalen of de gebruiker van telefoonnummer A, B en C een en dezelfde persoon is, los van het feit dat die persoon zich uitdrukt in taal D, E en F.

Met die software kan ook worden vastgesteld dat persoon X, die een maand geleden nummer A vanaf nummer D heeft opgebeld, dezelfde persoon is als degene die een maand later nummer B vanaf nummer Y heeft opgebeld.

Hulp bij het afluisteren – buiten het strikte kader van een gerechtelijk dossier / verband tussen verschillende gerechtelijke dossiers

De operationele context van dit scenario stemt overeen met de context van het voorgaande punt.

"Stemherkenning" wordt echter niet alleen gebruikt in het kader van het lopende gerechtelijke dossier, maar ook naar aanleiding van de analyse van de informatie die in het kader van een ander (lopend of afgesloten) gerechtelijk dossier werd ingewonnen.

Ces difficultés peuvent être illustrées de la sorte:

— Lorsque, dans le cadre d'un même dossier judiciaire, un ou divers appareils placés sous écoute sont utilisés par une multitude de personnes (parfois plus d'une dizaine);

— Lorsque, dans ce même cadre, les auteurs changent (ou s'échangent) régulièrement les cartes prépayées. A titre d'exemple, dans le cadre de dossiers judiciaires TEH (traite des êtres humains) actuellement en cours, la durée de vie moyenne d'une carte prépayée est de 48 heures.

Il n'est pas rare en outre, dans ce type de dossiers, que plusieurs dizaines de numéros soient successivement mis sous écoute.

Cette difficulté "d'identification" est rendue encore plus aiguë lorsque les personnes écoutées parlent une langue étrangère (voire plusieurs).

Dans ce cas, s'il y a une reconnaissance vocale celle-ci est réalisée *de facto* par le traducteur désigné.

Si les traductions sont faites par plusieurs traducteurs, cette reconnaissance est rendue encore plus aléatoire.

L'utilisation d'un logiciel de reconnaissance vocale permet à un officier de police judiciaire chargé d'une mesure d'interception, de déterminer facilement que l'utilisateur du numéro de téléphone A – B – C est la même personne et ce, indépendamment du fait que cette personne s'exprime tant en langue D, E et F.

Ce logiciel permettra aussi de constater que X, qui a appelé le numéro A avec un numéro D il y a un mois, est le même que celui qui a appelé le numéro B avec un numéro Y un mois plus tard.

Aide à l'écoute – en dehors du cadre strict du dossier judiciaire / lien entre divers dossiers judiciaires

Le contexte opérationnel de ce scénario est identique à celui décrit au point précédent.

Toutefois la "reconnaissance vocale" ne se fait pas uniquement dans le dossier judiciaire en cours mais résulte de l'analyse de l'information provenant d'un autre dossier judiciaire (en cours ou clôturé).

Een dergelijke scope mogelijk maken, heeft de volgende voordelen:

— het wordt mogelijk om eventuele verbanden tussen twee lopende gerechtelijke dossiers vast te stellen.

Zo kan een dossier inzake mensenhandel te Gent in verband worden gebracht met een dossier inzake mensenhandel te Brussel, enkel en alleen omdat is vastgesteld dat eenzelfde persoon in beide dossiers voorkomt.

— het wordt mogelijk om een onbekende in een dossier doeltreffender te identificeren (het wordt mogelijk om te stellen dat de spreker waarschijnlijk persoon X is) doordat die persoon daadwerkelijk geïdentificeerd is in het kader van een ander gerechtelijk dossier.

Op het niveau van de gegevensbank van stemafdrukken

De gegevensbank van stemafdrukken maakt deel uit van de Algemene Nationale Gegevensbank, waarvan de doeleinden zijn bepaald in artikel 44/7 van de wet op het politieambt. Deze gegevensbank moet immers een hulpmiddel zijn bij:

— de identificatie van de daders en verdachten die het onderwerp zijn of waren van een afluistermaatregel;

— de coördinatie en kruising van de persoonsgegevens en de politionele informatie.

De regels voor het beheer van de A.N.G. bepaald in de artikelen 44/7 tot 44/11/1 van de wet op het politieambt zijn dan ook van toepassing.

Daarbij kunnen wij inzonderheid vermelden dat:

— de bevoegde magistraat, met instemming van de federale procureur, kan beslissen om de voeding van de ANG met de stemafdrukken uit te stellen als die de uitoefening van de strafvordering of de veiligheid van een persoon in het gedrang kan brengen (conform artikel 44/8 WPA);

— De stemafdrukken kunnen ten hoogste tien jaar lang worden bewaard. Deze termijn is verzoenbaar met de algemene regel voor de persoonsgegevens verwerkt in de Algemene Nationale Gegevensbank (ANG) voor doeleinden van gerechtelijke politie. Artikel 44/9, § 2, eerste lid, a), 2° van de wet op het politieambt bepaalt namelijk dat deze gegevens worden gearchiveerd wanneer zij ontoereikend, niet ter zake dienend of overmatig van aard zijn, en in ieder geval na tien jaar voor wanbedrijven of na dertig jaar voor misdaden. Voor

Permettre un tel scope présente les avantages suivants:

— permettre l'établissement de liens éventuels entre deux dossiers judiciaires en cours.

Par exemple un dossier de traite des êtres humains à Gent pourrait est lié à un dossier TEH à Bruxelles, simplement par la constatation qu'une même personne intervient dans ces deux dossiers.

— permettre une identification plus effective d'un inconnu dans un dossier (permettre de dire que la personne qui parle est probablement X) grâce au fait que cette personne a été effectivement identifiée dans le cadre d'un autre dossier judiciaire.

Au niveau de la gestion de cette banque de données empreintes vocales

Cette banque de données des empreintes vocales fait partie de la Banque de données Nationale Générale, dont les finalités sont prévues à l'article 44/7 de la loi sur la fonction de police. Elle doit en effet permettre:

— d'aider à identifier les auteurs et les suspects qui ont fait ou font l'objet d'une mesure d'écoute;

— de coordonner et de croiser les données à caractère personnel et les informations policières.

Les règles de gestion de la B.N.G prévues dans les articles 44/7 à 44/11/1 de la loi sur la fonction de police sont donc d'application.

À ce titre, nous pouvons notamment mentionner que:

— le magistrat compétent, avec l'accord du procureur fédéral, peut décider de différer l'alimentation de la BNG avec les empreintes vocales si cela peut compromettre l'exercice de l'action publique ou la sécurité d'une personne (conformément à l'article 44/8 LFP);

— Les empreintes vocales peuvent être conservées au maximum dix ans. Ce délai est compatible avec la règle générale applicable aux données à caractère personnel dans la Banque de données Nationale Générale (BNG) à des fins de police judiciaire. L'article 44/9, § 2, alinéa 1er, a), 2°, de la loi sur la fonction de police précise en effet que ces données sont archivées lorsqu'elles présentent un caractère non adéquat, non pertinent ou excessif et en tout cas dix ans pour les délits et trente ans pour les crimes. En ce qui concerne les empreintes

stemafdrukken is een bewaartermijn van ten hoogste tien jaar aangewezen omdat de stem van de betrokkene nadien te zeer veranderd is.

— na die termijn worden de gegevens inzake de stemafdrukken gearchiveerd.

Ziehier, Dames en Heren, de draagwijdte van het ontwerp, dat de regering de eer heeft U ter goedkeuring voor te leggen.

De minister van Justitie,

Koen GEENS

vocales, un délai de conservation de dix ans maximum est indiqué. Au-delà, la voix de l'intéressé aura fortement changé.

— passé ce délai, les données relatives aux empreintes vocales sont archivées.

Voici, Mesdames, Messieurs, la portée du projet que le gouvernement a l'honneur de soumettre à votre approbation.

Le ministre de la Justice,

Koen GEENS

VOORONTWERP VAN WET

onderworpen aan het advies van de Raad van State

Voorontwerp van wet betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecommunicaties

TITEL 1

Algemene bepaling

Artikel 1

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

TITEL 2

Bepalingen tot wijziging van het Wetboek van Strafvordering

Artikel 2

In artikel 39*bis* van het Wetboek van Strafvordering, ingevoegd bij wet van 28 november 2000 en gewijzigd bij wet van 6 juni 2010, worden de volgende wijzigingen aangebracht:

1° In paragraaf 1 worden de woorden “of een deel ervan” ingevoegd tussen de woorden “een informaticasysteem” en de woorden “opgeslagen gegevens.”;

2° paragraaf 2 wordt vervangen als volgt:

“§ 2. Tot de zoeking in een informaticasysteem of een deel ervan dat wettelijk in beslag genomen is, kan beslist worden door een officier van gerechtelijke politie.

Onverminderd de exploitatie die voortvloeit uit de inbeslagname, kan de procureur des Konings of de arbeidsauditeur een zoeking bevelen in een informaticasysteem of een deel ervan dat door hem in beslag kan worden genomen.”;

3° Paragraaf 3 wordt vervangen als volgt:

“§ 3. Indien in de betrokken informaticasystemen opgeslagen gegevens aangetroffen worden die nuttig zijn voor dezelfde doeleinden als de inbeslagneming, maar de inbeslagneming van de drager daarvan evenwel niet wenselijk is, worden deze gegevens, evenals de gegevens noodzakelijk om deze te kunnen verstaan, gekopieerd op dragers, die toebehoren aan de overheid. In geval van dringendheid of om technische redenen, kan gebruik gemaakt worden van dragers, die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken.

AVANT-PROJET DE LOI

soumis à l’avis du Conseil d’État

Avant-projet de loi relative à l’amélioration des méthodes particulières de recherche et de certaines mesures d’enquête concernant Internet, les communications électroniques et les télécommunications

TITRE 1ER

Disposition générale

Article 1er

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

TITRE 2

Dispositions modifiant le Code d’Instruction criminelle

Article 2

A l’article 39*bis* du Code d’instruction criminelle, inséré par la loi du 28 novembre 2000 et modifié par la loi du 6 juin 2010, les modifications suivantes sont apportées:

1° Le paragraphe 1er est complété par les mots “ou une partie de celui-ci.”;

2° le paragraphe 2 est remplacé par ce qui suit:

“§ 2. La recherche dans un système informatique ou une partie de celui-ci qui a été légalement saisi, peut être décidée par un officier de police judiciaire.

Sans préjudice de l’exploitation découlant de la saisie, le procureur du Roi ou l’auditeur de travail peut ordonner une recherche dans un système informatique ou une partie de celui-ci qui peut être saisi par lui.”;

3° Le paragraphe 3 est remplacé par ce qui suit:

“§ 3. Si des données stockées sont trouvées dans les systèmes informatiques concernés qui sont utiles pour les mêmes finalités que celles prévues pour la saisie, mais que la saisie du support n’est néanmoins pas souhaitable, ces données, de même que les données nécessaires pour les comprendre, sont copiées sur des supports qui appartiennent à l’autorité. En cas d’urgence ou pour des raisons techniques, il peut être fait usage de supports qui sont disponibles pour des personnes autorisées à utiliser le système informatique.

Bovendien worden passende technische middelen aangewend om de toegang tot deze gegevens in het informaticasysteem, evenals tot de kopieën daarvan die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken, te verhinderen en hun integriteit te waarborgen.

Wanneer de in het eerste lid vermelde maatregel niet mogelijk is om technische redenen of wegens de omvang van de gegevens, wendt hij de passende technische middelen aan om de toegang tot deze gegevens in het informaticasysteem, evenals tot de kopieën daarvan die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken, te verhinderen en hun integriteit te waarborgen.

Indien de gegevens het voorwerp van het misdrijf vormen of voortgekomen zijn uit het misdrijf en indien de gegevens strijdig zijn met de openbare orde of de goede zeden, of een gevaar opleveren voor de integriteit van informaticasystemen of gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen, wendt de procureur des Konings of de arbeidsauditeur alle passende technische middelen aan om deze gegevens ontoegankelijk te maken of, na hiervan kopie te hebben genomen, te verwijderen.

Hij kan evenwel, behoudens in het geval bedoeld in het vorige lid, het verdere gebruik van het geheel of een deel van deze gegevens toestaan, wanneer dit geen gevaar voor de strafvordering oplevert.

In geval van uiterst dringende noodzakelijkheid en wanneer het kennelijk gaat om een strafbaar feit zoals bedoeld in artikel 383*bis*, § 1, van het Strafwetboek, kan de procureur des Konings mondeling bevelen dat alle passende technische middelen worden aangewend om de gegevens, die het voorwerp van het misdrijf vormen of voortgekomen zijn uit het misdrijf en die strijdig zijn met de openbare orde of de goede zeden, ontoegankelijk te maken. Dit bevel wordt zo spoedig mogelijk schriftelijk bevestigd, met vermelding van de redenen van de uiterst dringende noodzakelijkheid.";

4° paragraaf 4 wordt vervangen als volgt:

"§ 4. De procureur des Konings of de arbeidsauditeur kan de zoeking in een informaticasysteem of een deel ervan uitbreiden naar een informaticasysteem of een deel daarvan dat zich op een andere plaats bevindt dan daar waar de zoeking plaatsvindt:

— indien deze uitbreiding noodzakelijk is om de waarheid aan het licht te brengen ten aanzien van het misdrijf dat het voorwerp uitmaakt van de zoeking; en

— indien andere maatregelen disproportioneel zouden zijn, of indien er een risico bestaat dat zonder deze uitbreiding bewijselementen verloren gaan.

De uitbreiding van de zoeking in een informaticasysteem mag zich niet verder uitstrekken dan tot de informaticasystemen of de delen daarvan waartoe de personen die gerechtigd zijn het onderzochte informaticasysteem te gebruiken, in het bijzonder toegang hebben.

On utilise en outre les moyens techniques appropriés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité.

Lorsque la mesure prévue au § 2 n'est pas possible, pour des raisons techniques ou à cause du volume des données, le procureur du Roi utilise les moyens techniques appropriés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité.

Si les données forment l'objet de l'infraction ou ont été produites par l'infraction et si elles sont contraires à l'ordre public ou aux bonnes mœurs ou constituent un danger pour l'intégrité des systèmes informatiques ou pour des données stockées, traitées ou transmises par le biais de tels systèmes, le procureur du Roi ou l'auditeur du travail utilise tous les moyens techniques appropriés pour rendre ces données inaccessibles ou, après en avoir pris copie, les retirer.

Il peut cependant, sauf dans le cas prévu à l'alinéa précédent, autoriser l'usage ultérieur de l'ensemble ou d'une partie de ces données, lorsque cela ne présente pas de danger pour l'exercice des poursuites.

En cas d'extrême urgence et s'il s'agit manifestement d'une infraction visée à l'article 383*bis*, § 1er, du Code pénal, le procureur du Roi peut ordonner verbalement que tous les moyens appropriés soient utilisés pour rendre inaccessibles les données qui forment l'objet de l'infraction ou ont été produites par l'infraction et qui sont contraires à l'ordre public ou aux bonnes mœurs. Cet ordre est confirmé par écrit dans les meilleurs délais, avec mention des motifs de l'extrême urgence.";

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

"§ 4. Le procureur du Roi ou l'auditeur de travail peut étendre la recherche dans un système informatique ou une partie de celui-ci vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée:

— si cette extension est nécessaire pour la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche; et

— si d'autres mesures seraient disproportionnées, ou s'il existe un risque que, sans cette extension, des éléments de preuve soient perdus.

L'extension de la recherche dans un système informatique ne peut pas excéder les systèmes informatiques ou les parties de tels systèmes auxquels les personnes autorisées à utiliser le système informatique qui fait l'objet de la mesure ont spécifiquement accès.

Inzake de door uitbreiding van de zoeking in een informaticasysteem aangetroffen gegevens, die nuttig zijn voor dezelfde doeleinden als de inbeslagneming, wordt gehandeld zoals bepaald in § 3.

Wanneer blijkt dat deze gegevens zich niet op het grondgebied van het Rijk bevinden, worden ze enkel gekopieerd. In dat geval deelt de procureur des Konings of de arbeidsauditeur dit onverwijld mee aan de Federale Overheidsdienst Justitie, die de bevoegde overheid van de betrokken Staat hiervan op de hoogte brengt, indien deze redelijkerwijze kan worden bepaald.

Indien de uitbreiding van een zoeking in een informaticasysteem wordt bevolen door de onderzoeksrechter, kan hij die opdracht geven aan een officier van gerechtelijke politie van zijn arrondissement of van het arrondissement waar de handelingen moeten plaatshebben. Wanneer de onderzoeksrechter optreedt op vordering van een onderzoeksrechter van een ander arrondissement, kan hij opdracht geven aan een officier van gerechtelijke politie van dat ander arrondissement.

In geval van uiterst dringende noodzakelijkheid of in geval van heterdaad kan de procureur des Konings of de arbeidsauditeur de uitbreiding van de zoeking bedoeld in het eerste lid mondeling bevelen. Dit bevel wordt zo spoedig mogelijk schriftelijk bevestigd, met vermelding van de heterdaadsituatie of van de redenen van de uiterst dringende noodzakelijkheid.";

5° er wordt een paragraaf 4*bis* ingevoegd, luidende:

"§ 4*bis*. Enkel de onderzoeksrechter kan, overeenkomstig de voorwaarden voorzien in paragraaf 4, een andere zoeking bevelen in een informaticasysteem of een deel ervan dan de zoekingen voorzien in de paragrafen 2 en 4.";

6° er wordt een paragraaf 4*ter* ingevoegd, luidende:

"§ 4*ter*. Teneinde de maatregelen bedoeld in dit artikel mogelijk te maken, kan de procureur des Konings, de arbeidsauditeur of de onderzoeksrechter bevelen om, te allen tijde, ook zonder de toestemming van hetzij de eigenaar of zijn rechthebbende, hetzij de gebruiker:

— elke beveiliging van de betrokken informaticasystemen tijdelijk op te heffen, desgevallend met behulp van technische hulpmiddelen, valse signalen, valse sleutels of valse hoedanigheden;

— technische middelen in de betrokken informaticasystemen aan te brengen teneinde de door dat systeem opgeslagen, verwerkte of doorgestuurde gegevens te ontcijferen en te decoderen.

Evenwel kan enkel de onderzoeksrechter deze tijdelijke opheffing van de beveiliging of deze aanbrenging van technische middelen bevelen wanneer dit in het bijzonder noodzakelijk is voor de toepassing van paragraaf 4.";

En ce qui concerne les données recueillies par l'extension de la recherche dans un système informatique, qui sont utiles pour les mêmes finalités que celles prévues pour la saisie, les règles prévues au § 3 s'appliquent.

Lorsqu'il s'avère que ces données ne se trouvent pas sur le territoire du Royaume, elles peuvent seulement être copiées. Dans ce cas, le procureur du Roi ou l'auditeur du travail communique sans délai cette information au Service public fédéral Justice, qui en informe les autorités compétentes de l'état concerné, si celui-ci peut raisonnablement être déterminée.

Si l'extension d'une recherche dans un système informatique est ordonnée par le juge d'instruction, celui-ci peut déléguer un officier de police judiciaire de son arrondissement ou de l'arrondissement où les actes doivent avoir lieu. Lorsque le juge d'instruction agit sur la réquisition d'un juge d'instruction d'un autre arrondissement, il peut déléguer un officier de police judiciaire de cet autre arrondissement.

En cas d'extrême urgence ou de flagrant délit, le procureur du Roi ou l'auditeur du travail peut ordonner verbalement l'extension de la recherche visée à l'alinéa 1er. Cet ordre est confirmé par écrit dans les meilleurs délais, avec mention du flagrant délit ou des motifs de l'extrême urgence.";

5° il est inséré un paragraphe 4*bis*, rédigé comme suit:

"§ 4*bis*. Seul le juge d'instruction peut ordonner, selon les conditions visées au paragraphe 4, une recherche dans un système informatique ou une partie de celui-ci autre que les recherches visées aux paragraphes 2 et 4.";

6° il est inséré un paragraphe 4*ter*, rédigé comme suit:

"§ 4*ter*. En vue de permettre les mesures visée à cet article, le procureur du Roi, l'auditeur de travail ou le juge d'instruction peut également, sans le consentement du propriétaire ou de son ayant droit, ou de l'utilisateur, ordonner, à tout moment:

— la suppression temporaire de toute protection des systèmes informatiques concernés, le cas échéant à l'aide de moyens techniques, de faux signaux, de fausses clés ou de fausses qualités;

— l'installation de dispositifs techniques dans les systèmes informatiques concernés en vue du décryptage et du décodage de données stockées, traitées ou transmises par ce système.

Toutefois, seul le juge d'instruction peut ordonner cette suppression temporaire de protection ou cette installation de dispositifs techniques lorsque ceci est spécifiquement nécessaire pour l'application du paragraphe 4.";

7° paragraaf 5 wordt vervangen als volgt:

"§ 5. De procureur des Konings of de arbeidsauditeur brengt de verantwoordelijke van het informaticasysteem op de hoogte van de zoeking in het informaticasysteem of de uitbreiding ervan, tenzij diens identiteit of woonplaats redelijkerwijze niet achterhaald kan worden, en deelt hem in voorkomend geval een samenvatting mee van de gegevens die zijn gekopieerd, ontoegankelijk gemaakt of verwijderd.".

Artikel 3

In hetzelfde Wetboek wordt een artikel 39*ter* ingevoegd, luidende:

"Art. 39*ter*. § 1. Bij het opsporen van de misdaden en de wanbedrijven en onverminderd de bevoegdheden bedoeld in de artikelen 39*bis*, 46*bis* en 88*bis* van het Wetboek van strafvordering en de artikelen XII.17, XII.18, XII.19 en XII.20 van het Wetboek van Economisch Recht, kan iedere officier van gerechtelijke politie, wanneer er redenen bestaan om aan te nemen dat gegevens die opgeslagen, verwerkt of overgedragen worden door middel van een informaticasysteem bijzonder kwetsbaar zijn voor verlies of voor wijziging, bij een gemotiveerde en schriftelijke beslissing aan een of meerdere natuurlijke personen of rechtspersonen bevelen de gegevens die in hun bezit zijn of waarover zij controle hebben te bewaren.

De gemotiveerde en schriftelijke beslissing vermeldt:

— de naam en hoedanigheid van de officier van gerechtelijke politie die om de bewaring verzoekt;

— het strafbare feit waarop het verzoek betrekking heeft;

— de gegevens die bewaard moeten worden;

— de duur van bewaring van de gegevens, die niet langer mag zijn dan negentig dagen. Deze termijn kan schriftelijk worden verlengd.

In spoedeisende gevallen kan de opdracht tot bewaring mondeling worden gegeven. De opdracht moet zo spoedig mogelijk worden bevestigd in de vorm bepaald in het vorige lid.

§ 2. De natuurlijke personen of rechtspersonen bedoeld in § 1, zorgen ervoor dat de integriteit van de gegevens gewaarborgd is en dat de gegevens op een veilige manier bewaard worden.

§ 3. Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

Iedere persoon die weigert mee te werken, of die de bewaarde gegevens doet verdwijnen, vernietigt of wijzigt, wordt

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

"§ 5. Le procureur du Roi ou l'auditeur du travail informe le responsable du système informatique de la recherche effectuée dans le système informatique ou de son extension, sauf si son identité ou son adresse ne peuvent être raisonnablement retrouvées, et lui communique le cas échéant un résumé des données qui ont été copiées, rendues inaccessibles ou retirées.".

Article 3

Dans le même Code, il est inséré un article 39*ter* rédigé comme suit:

"Art. 39*ter*. § 1er. Lors de la recherche de crimes et délits et sans préjudice des compétences visées aux articles 39*bis*, 46*bis* et 88*bis* du Code d'instruction criminelle et aux articles XII.17, XII.18, XII.19 et XII.20 du Code de droit économique, tout officier de police judiciaire peut, s'il existe des raisons de croire que des données stockées, traitées ou transmises par un système informatique au moyen d'un système informatique sont particulièrement susceptibles de perte ou de modification, ordonner, par une décision écrite motivée, à une ou plusieurs personnes physiques ou personnes morales de conserver les données qui sont en leur possession ou sous leur contrôle.

La décision écrite motivée mentionne:

— les nom et qualité de l'officier de police judiciaire commis pour l'exécution de la mesure;

— l'infraction qui fait l'objet de la recherche;

— les données qui doivent être conservées;

— la durée de conservation des données, qui ne peut excéder nonante jours. Ce délai peut être prolongé par écrit.

En cas d'urgence, la conservation peut être ordonnée verbalement. Elle doit être confirmée dans les plus brefs délais dans la forme prévue à l'alinéa précédent.

§ 2. Les personnes physiques ou personnes morales visées au § 1er veillent à ce que l'intégrité des données soit garantie et à ce que les données soient conservées de manière sécurisée.

§ 3. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

Toute personne qui refuse de coopérer, ou qui fait disparaître, détruit ou modifie les données conservées, sera punie

gestraft met een gevangenisstraf van zes maanden tot een jaar en met een geldboete van 26 tot 20 000 euro of met één van die straffen alleen.

§ 4. De bewaarde gegevens dienen volgens de toepasselijke wetsbepalingen overgemaakt te worden aan de bevoegde gerechtelijke autoriteit.".

Artikel 4

In hetzelfde Wetboek wordt een artikel 39*quater* ingevoegd, luidende:

"Art. 39*quater*. § 1. Onverminderd de mogelijkheden tot rechtstreekse samenwerking met buitenlandse operatoren van elektronische communicatienetwerken en verstrekkers van elektronische communicatiediensten, kan de procureur des Konings, via de door de minister van Justitie aangewezen politiedienst, aan een buitenlandse bevoegde autoriteit verzoeken de snelle bewaring te bevelen of op andere wijze op te leggen van gegevens die opgeslagen, verwerkt of overgedragen worden door middel van een informaticasysteem dat zich bevindt op het grondgebied van die bevoegde autoriteit en ten aanzien waarvan een Belgische bevoegde gerechtelijke autoriteit voornemens is een verzoek om rechtshulp in te dienen.

Het verzoek om bewaring is schriftelijk en vermeldt:

— de naam en hoedanigheid van de autoriteit die om de bewaring verzoekt;

— het strafbare feit waarop het verzoek betrekking heeft en een korte uiteenzetting van de daarop betrekking hebbende feiten;

— de gegevens die bewaard moeten worden en het verband met het strafbare feit;

— alle beschikbare informatie met betrekking tot de bewaarder van de gegevens of de locatie van het informaticasysteem;

— de noodzaak van de bewaring;

— het feit dat een verzoek om rechtshulp ingediend zal worden met betrekking tot de bewaarde gegevens;

— in voorkomend geval, het feit dat de gegevens die bewaard moeten worden verwijzen naar een andere staat dan de staat van de bevoegde buitenlandse autoriteit.

§ 2. Indien een internationaal rechtsinstrument tussen België en een andere Staat hierin voorziet, kan een bevoegde autoriteit van die Staat aan de door de minister van Justitie aangewezen politiedienst verzoeken de snelle bewaring te bevelen of op andere wijze op te leggen van gegevens die zich bevinden op het Belgische grondgebied en ten aanzien waarvan deze buitenlandse autoriteit voornemens is een verzoek om rechtshulp in te dienen.

d'un emprisonnement de six mois à un an ou d'une amende de 26 euros à 20 000 euros ou d'une de ces peines seulement.

§ 4. Les données conservées doivent être transmises à l'autorité judiciaire compétente selon les dispositions légales applicables.".

Article 4

Dans le même Code, il est inséré un article 39*quater* rédigé comme suit:

"Art. 39*quater*. § 1er. Sans préjudice des possibilités de collaboration directe avec des opérateurs de services de communications électroniques et des fournisseurs de services de communications électroniques étrangers, le procureur du Roi peut, par l'intermédiaire du service de police désigné par le ministre de la Justice, demander à une autorité compétente étrangère d'ordonner ou d'imposer d'une autre façon la conservation rapide de données stockées, traitées ou transmises par un système informatique qui se trouvent sur le territoire de cette autorité compétente et au sujet desquelles une autorité judiciaire belge compétente a l'intention de soumettre une demande d'entraide judiciaire.

La demande de conservation est formulée par écrit et mentionne:

— les nom et qualité de l'autorité qui demande la conservation;

— l'infraction qui fait l'objet de la demande et un exposé succinct des faits qui y ont trait;

— les données à conserver et le lien avec l'infraction;

— toutes les informations disponibles concernant le dépositaire des données ou la localisation du système informatique;

— la nécessité de la conservation;

— le fait qu'une demande d'entraide judiciaire concernant les données conservées sera soumise;

— le cas échéant, le fait que les données qui doivent être conservées renvoient à un autre État que l'État de l'autorité étrangère compétente.

§ 2. Lorsqu'une telle possibilité est prévue dans un instrument de droit international liant la Belgique et un autre État, une autorité compétente de cet État peut demander au service de police désigné par le ministre de la Justice d'ordonner ou d'imposer d'une autre manière la conservation rapide de données stockées, traitées ou transmises par un système informatique qui se trouvent sur le territoire belge et au sujet desquelles cette autorité judiciaire étrangère a l'intention de soumettre une demande d'entraide judiciaire.

Het verzoek om bewaring is schriftelijk en vermeldt:

— de naam en hoedanigheid van de autoriteit die om de bewaring verzoekt;

— het strafbare feit waarop het verzoek betrekking heeft en een korte uiteenzetting van de daarop betrekking hebbende feiten;

— de gegevens die bewaard moeten worden en het verband met het strafbare feit;

— alle beschikbare informatie met betrekking tot de bewaarder van de gegevens of de locatie van het informaticasysteem;

— de noodzaak van de bewaring, en

— het feit dat een verzoek om rechtshulp ingediend zal worden met betrekking tot de bewaarde gegevens;

— in voorkomend geval, het feit dat de gegevens die bewaard moeten worden verwijzen naar een andere staat dan de staat van de bevoegde buitenlandse autoriteit.

Na ontvangst van het verzoek bedoeld in het vorige lid, brengt de in het eerste lid bedoelde politiedienst de bevoegde procureur des Konings of onderzoeksrechter daarvan op de hoogte, en neemt zij alle passende maatregelen om onverwijld over te gaan tot de snelle bewaring van de nader omschreven gegevens, overeenkomstig artikel 39*ter*.

Onverminderd de internationale rechtsinstrumenten met betrekking tot rechtshulp waardoor België gebonden is en die ertoe strekken deze samenwerking te bevorderen, kan een verzoek om bewaring door de bevoegde procureur des Konings of onderzoeksrechter alleen worden geweigerd indien:

— het verzoek betrekking heeft op een misdrijf dat door België wordt beschouwd als politiek misdrijf of als een met een politiek misdrijf samenhangend feit, of

— de uitvoering van het verzoek zou kunnen leiden tot aantasting van de soevereiniteit, veiligheid, openbare orde of andere wezenlijke belangen van België.

Wanneer de in het eerste lid bedoelde politiedienst van mening is dat de gewone bewaring de toekomstige beschikbaarheid van de gegevens niet waarborgt of de vertrouwelijkheid van het onderzoek van de bevoegde buitenlandse autoriteit in gevaar brengt of dit anderszins schaadt, brengt zij de bevoegde buitenlandse autoriteit hiervan onverwijld op de hoogte, die vervolgens bepaalt of het verzoek niettemin moet worden uitgevoerd.

Een bewaring verricht in antwoord op het in het eerste lid bedoelde verzoek is geldig voor een periode van ten minste 60 dagen, teneinde de bevoegde buitenlandse autoriteit de mogelijkheid te bieden een verzoek om rechtshulp in te

La demande de conservation est formulée par écrit et mentionne:

— les nom et qualité de l'autorité qui demande la conservation;

— l'infraction qui fait l'objet de la demande et un exposé succinct des faits qui y ont trait;

— les données à conserver et le lien avec l'infraction;

— toutes les informations disponibles concernant le dépositaire des données ou la localisation du système informatique;

— la nécessité de la conservation, et

— le fait qu'une demande d'entraide judiciaire concernant les données conservées sera soumise;

— le cas échéant, le fait que les données qui doivent être conservées renvoient à un autre État que l'État de l'autorité étrangère compétente.

Après réception de la demande visée à l'alinéa précédent, le service de police visé à l'alinéa 1er en informe le procureur du Roi ou le juge d'instruction compétent et prend toutes les mesures appropriées pour procéder sans délai à la conservation rapide des données définies conformément à l'article 39*ter*.

Sans préjudice des instruments de droit international liant la Belgique en matière d'entraide judiciaire et tendant à promouvoir celle-ci, une demande de conservation peut être rejetée à tout moment par le procureur du Roi ou le juge d'instruction compétent:

— si la demande concerne une infraction considérée par la Belgique comme une infraction politique ou un fait connexe à une infraction politique, ou

— si l'exécution de la demande est de nature à por*ter* atteinte à la souveraineté, à la sécurité, à l'ordre public ou à d'autres intérêts essentiels de la Belgique.

Si le service de police visé à l'alinéa 1er estime que la conservation simple ne suffira pas à garantir la disponibilité future des données, ou compromettra la confidentialité de l'enquête de l'autorité étrangère compétente ou nuira d'une autre façon à celle-ci, il en informe sans délai l'autorité étrangère compétente, qui décide alors s'il convient néanmoins d'exécuter la demande.

Une conservation effectuée en réponse à la demande visée à l'alinéa 1er est valable pour une période d'au moins 60 jours afin d'offrir à l'autorité étrangère compétente la possibilité de soumettre une demande d'entraide judiciaire. Après réception

dienen. Na de ontvangst van een dergelijk verzoek blijven de gegevens bewaard in afwachting van een beslissing inzake het verzoek.

Indien de gegevens die opgeslagen, verwerkt of overgedragen worden door middel van een informaticasysteem verwijzen naar een andere staat dan de staat van de verzoekende bevoegde buitenlandse autoriteit, brengt de in het eerste lid bedoelde politiedienst de bevoegde procureur des Konings of onderzoeksrechter daarvan op de hoogte. Deze gaat zo snel mogelijk over tot de onthulling aan de bevoegde buitenlandse autoriteit van een hoeveelheid identificatiegegevens of oproepgegevens voldoende om te achterhalen wie die operator van het elektronische communicatienetwerk of de verstrekker van de elektronische communicatiedienst is en langs welke weg de communicatie was verzonden.".

Artikel 5

In artikel 46*bis* van hetzelfde Wetboek, ingevoegd bij wet van 10 juni 1998 en gewijzigd bij de wetten van 27 december 2004, 23 januari 2007 en … (dataretentiewet) worden de volgende wijzigingen aangebracht:

1° paragraaf 1 wordt vervangen als volgt:

"§ 1. Bij het opsporen van de misdaden en wanbedrijven kan de procureur des Konings bij een gemotiveerde en schriftelijke beslissing overgaan of doen overgaan op basis van ieder gegeven in zijn bezit of door middel van een toegang tot de klantenbestanden van de actoren bedoeld in het tweede lid, eerste en tweede streepje, tot:

1° de identificatie van de abonnee of de gewoonlijke gebruiker van een dienst zoals bedoeld in het tweede lid, tweede streepje, of van het gebruikte elektronische communicatiemiddel;

2° de identificatie van de diensten zoals bedoeld in het tweede lid, tweede streepje, waarop een bepaald persoon geabonneerd is of die door een bepaald persoon gewoonlijk gebruikt worden.

Hiertoe kan hij zo nodig, rechtstreeks of via de door de Koning aangewezen politiedienst, de medewerking vorderen van:

— de operator van een elektronisch communicatienetwerk; en

— iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.

De motivering weerspiegelt de proportionaliteit met inachtneming van de persoonlijke levenssfeer en de subsidiariteit ten opzichte van elke andere onderzoeksdaad.

d'une telle demande, les données restent conservées dans l'attente d'une décision concernant la demande.

Si les données qui sont stockées, traitées ou transmises par un système informatique renvoient à un autre État que l'État de l'autorité étrangère compétente requérante, le service de police visé à l'alinéa 1er en informe le procureur du Roi ou le juge d'instruction compétent. Celui-ci divulgue, dans les meilleurs délais, à l'autorité étrangère compétente une quantité de données d'identification ou d'appel suffisante pour retrouver qui est l'opérateur du réseau de communications électroniques ou le fournisseur du service de communications électroniques et par quelle voie la communication a été envoyée.".

Article 5

A l'article 46*bis* du même Code, inséré par la loi du 10 juin 1998 et modifié par les lois du 27 décembre 2004, 23 janvier 2007 et … (loi dataretention) les modifications suivantes sont apportées:

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

"§ 1er. En recherchant les crimes et les délits, le procureur du Roi peut, par une décision motivée et écrite, procéder ou faire procéder sur la base de toutes données détenues par lui, ou au moyen d'un accès aux fichiers des clients des acteurs visés à l'alinéa 2, 1er et 2e tirets, à

1° l'identification de l'abonné ou de l'utilisateur habituel d'un service visé à l'alinéa 2, deuxième tiret, ou bien du moyen de communication électronique utilisé;

2° l'identification des services visés à l'alinéa 2, deuxième tiret, auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée.

Si nécessaire, il peut pour ce faire requérir, directement ou par l'intermédiaire d'un service de police désigné par le Roi, la collaboration:

— de l'opérateur d'un réseau de communications électroniques;

— de toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.

La motivation reflète le caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête.

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, rechtstreeks of via de tussenkomst van een politiedienst aangewezen door de Koning, 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.

Voor strafbare feiten die geen correctionele hoofdgevangenisstraf van een 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.";

2° in paragraaf 2 wordt het eerste lid vervangen als volgt:

"De actoren bedoeld in § 1, tweede lid, eerste en tweede streepje, van wie gevorderd wordt de in paragraaf 1 bedoelde gegevens mee te delen, verstrekken de procureur des Konings of de officier van gerechtelijke politie de gegevens die werden opgevraagd in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, termijn waarvan de modaliteiten vastgesteld worden door de Koning, op het voorstel van de minister van Justitie en de minister bevoegd voor Telecommunicatie.";

3° in paragraaf 2 wordt het laatste lid vervangen als volgt:

"Iedere persoon die de gegevens weigert mee te delen of niet meedeelt in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, wordt gestraft met geldboete van zesentwintig euro tot tienduizend euro.".

Artikel 6

In artikel 46*quinquies* van hetzelfde Wetboek, ingevoegd bij wet van 27 december 2005, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1 worden de woorden ", met inbegrip van het openen van gesloten voorwerpen die zich op deze plaats bevinden" ingevoegd tussen de woorden "een private plaats te betreden" en de woorden ", wanneer er ernstige aanwijzingen zijn";

2° in paragraaf 2 worden de woorden "betreden van de private plaats zoals bedoeld in § 1" vervangen door de woorden "betreden van de private plaats zoals bedoeld in § 1, met inbegrip van het openen van gesloten voorwerpen die zich op deze plaats bevinden,";

3° in paragraaf 2 wordt de bepaling onder 3°, aangevuld met de woorden ", te herstellen of terug te nemen;";

En cas d'extrême urgence, chaque officier de police judiciaire peut, avec l'accord verbal et préalable du procureur du Roi, et par une décision motivée et écrite requérir directement ou par l'intermédiaire d'un service de police désigné par le Roi, 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 qui ne sont pas de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde, le procureur du Roi ne peut requérir les données visées à l'alinéa 1er que pour une période de six mois préalable à sa décision.";

2° dans le paragraphe 2, le premier alinéa est remplacé par ce qui suit:

"Les acteurs visés au § 1er, alinéa 2, 1er et 2e tirets, requis de communiquer les données visées au § 1er fournissent au procureur du Roi ou à l'officier de police judiciaire les données qui ont été demandées en temps réel ou, le cas échéant, au moment précisé dans la réquisition, délai dont les modalités sont fixées par le Roi, sur la proposition du ministre de la Justice et du ministre compétent pour les Télécommunications.";

3° dans le paragraphe 2, le dernier alinéa est remplacé par ce qui suit:

"Toute personne qui refuse de communiquer les données ou qui ne les communique pas en temps réel ou, le cas échéant, au moment précisé dans la réquisition est punie d'une amende de vingt-six euros à dix mille euros.".

Article 6

A l'article 46*quinquies* du même Code, inséré par la loi du 27 décembre 2005, les modifications suivantes sont apportées:

1° dans le paragraphe premier, les mots ", en ce compris ouvrir les objets fermés se trouvant dans ce lieu," sont insérés entre les mots "à tout moment dans un lieu privé" et "à l'insu du propriétaire";

2° dans le paragraphe 2, les mots "pénétration du lieu privé visé au § 1er," sont remplacés par les mots "pénétration du lieu privé visé au § 1er, en ce compris l'ouverture des objets fermés se trouvant sur ce lieu,";

3° dans le paragraphe 2, le 3° est remplacé par ce qui suit: "3° de réparer ou de retirer dans le cadre d'une observation un moyen technique visé à l'article 47*sexies*, § 1er, alinéa 3;";

4° paragraaf 2 wordt aangevuld met de bepaling onder 4°, luidende:

"4° de overeenkomstig § 5 meegenomen voorwerpen terug te plaatsen.";

5° het artikel wordt aangevuld met de paragrafen 5, 6 en 7 luidende:

"§ 5. Indien het onderzoek van een in § 1 bedoeld voorwerp niet ter plaatse kan gebeuren en indien de informatie niet op een andere manier kan worden verkregen, is het de politiedienst toegestaan dit voorwerp mee te nemen voor een strikt beperkte duur. Het bewuste voorwerp wordt zo spoedig mogelijk teruggeplaatst, tenzij dit het goede verloop van het onderzoek in de weg staat.

§ 6. In het kader van de maatregel bedoeld in § 1, is het binnendringen in een informaticasysteem enkel mogelijk met het oog op de doeleinden bedoeld in § 2, 3°.

§ 7. De officier van gerechtelijke politie die de leiding heeft over de uitvoering van de maatregel bedoeld in § 1 of in artikel 89*ter*, § 1, stelt van het verloop van de maatregel een procesverbaal op. Wanneer tijdens de uitvoering van de maatregel gesloten voorwerpen geopend werden of toepassing gemaakt werd van § 5, wordt daarvan melding gemaakt in het procesverbaal. Het proces-verbaal wordt uiterlijk na het beëindigen van de maatregel bij het strafdossier gevoegd."

Artikel 7

In hetzelfde Wetboek wordt een nieuw artikel 46*sexies* ingevoegd, luidende:

"Art. 46*sexies*. § 1. Bij het opsporen van de misdaden en de wanbedrijven, wanneer het onderzoek zulks vereist en de overige middelen van onderzoek niet lijken te volstaan om de waarheid aan de dag te brengen, kan de procureur des Konings de door de minister van Justitie aangewezen politiediensten machtigen om op het internet, desgevallend onder een fictieve identiteit, contact te onderhouden met een of meerdere personen waarvan er ernstige aanwijzingen zijn dat zij strafbare feiten die een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben, plegen of zouden plegen.

In uitzonderlijke omstandigheden en mits uitdrukkelijke machtiging van de procureur des Konings, kan de in het eerste lid bedoelde politieambtenaar bij een welbepaalde operatie kortstondig een beroep doen op de deskundigheid van een persoon die niet tot de politiediensten behoort, indien dit strikt noodzakelijk voorkomt voor het welslagen van zijn opdracht.

Dit artikel is niet van toepassing op de persoonlijke interactie op het internet van politieambtenaren met een of meerdere personen, die enkel een gerichte verificatie of een arrestatie tot direct doel heeft.

§ 2. De maatregel bedoeld in § 1 kan door de procureur des Konings bevolen worden met een voorafgaandelijke en met

4° le paragraphe 2 est complété par le 4° rédigé comme suit:

"4º de replacer les objets emportés conformément au § 5.";

5° l'article est complété par les paragraphes 5,6 et 7, rédigés comme suit:

"§ 5. Si l'examen d'un objet visé au § 1er ne peut se faire sur place et si l'information ne peut être obtenue d'une autre manière, le service de police est autorisé à empor*ter* cet objet pour une durée strictement limitée. L'objet en question est remis en place dans les plus brefs délais, à moins que cela n'entrave le bon déroulement de l'enquête.

§ 6. Dans le cadre de la mesure visée au § 1er, la pénétration dans un système informatique n'est possible qu'aux fins visées au § 2, 3°.

§ 7. L'officier de police judiciaire qui dirige l'exécution de la mesure visé au § 1er ou à l'article 89*ter*, § 1er, rédige un procès-verbal du cours de la mesure. Lorsque des objets fermés sont ouverts ou qu'il est fait application du § 5 durant l'exécution de la mesure, il en est fait mention dans le procès-verbal. Le procès-verbal est joint au dossier répressif au plus tard après qu'il a été mis fin à la mesure."

Article 7

Dans le même Code, il est inséré un article 46*sexies* rédigé comme suit:

"Art. 46*sexies*. § 1er. Dans la recherche des crimes et délits, si les nécessités de l'enquête l'exigent et que les autres moyens d'investigation ne semblent pas suffire à la manifestation de la vérité, le procureur du Roi peut autoriser les services de police désignés par le ministre de la Justice à entretenir, le cas échéant sous une identité fictive, des contacts avec une ou plusieurs personnes concernant lesquelles il existe des indices sérieux qu'elles commettent ou commettraient des infractions pouvant donner lieu à un emprisonnement correctionnel principal d'un an ou à une peine plus lourde.

Dans des circonstances exceptionnelles et moyennant l'autorisation expresse du procureur du Roi, le fonctionnaire de police visé à l'alinéa 1er peut, dans le cadre d'une opération déterminée, momentanément recourir à l'expertise d'une personne qui ne fait pas partie des services de police si cela s'avère strictement nécessaire à la réussite de sa mission.

Le présent article ne s'applique pas à l'interaction personnelle de fonctionnaires de police avec une ou plusieurs personnes sur Internet, qui n'a pour finalité directe qu'une vérification ciblée ou une arrestation.

§ 2. La mission visée au § 1er peut être ordonnée par le procureur du Roi par une autorisation écrite et motivée préalable.

redenen omklede schriftelijke machtiging. Deze machtiging is geldig voor een termijn van drie maanden, onverminderd hernieuwing.

In spoedeisende gevallen kan de machtiging mondeling worden verstrekt. De machtiging moet zo spoedig mogelijk worden bevestigd in de vorm bepaald in het eerste lid.

§ 3. Blijven vrij van straf de politieambtenaren die, in het kader van hun opdracht en met het oog op het welslagen ervan of ter verzekering van hun eigen veiligheid of deze van andere bij de maatregel betrokken personen, strikt noodzakelijke strafbare feiten plegen, mits uitdrukkelijk akkoord van de procureur des Konings.

Die strafbare feiten mogen niet ernstiger zijn dan die waarvoor de maatregel wordt aangewend en moeten noodzakelijkerwijze evenredig zijn met het nagestreefde doel.

Het eerste en het tweede lid zijn eveneens van toepassing op de personen die aan de uitvoering van deze opdracht noodzakelijke en rechtstreekse hulp of bijstand hebben verleend en op de personen, bedoeld in § 1, tweede lid.

Blijft vrij van straf de magistraat die, met inachtneming van dit wetboek, machtiging verleent aan een politieambtenaar en aan de personen bedoeld in het derde lid tot het plegen van strafbare feiten in het kader van de uitvoering van de maatregel.

De politieambtenaren melden schriftelijk en vóór de uitvoering van de maatregel aan de procureur des Konings, de misdrijven die zij of de personen bedoeld in het derde lid, voornemens zijn te plegen.

Indien deze voorafgaande kennisgeving niet kon gebeuren, stellen de politieambtenaren de procureur des Konings onverwijld in kennis van de misdrijven die zij of de personen bedoeld in het derde lid, hebben gepleegd en bevestigen dit nadien schriftelijk.

De procureur des Konings vermeldt in een afzonderlijke en schriftelijke beslissing de misdrijven die door de politiediensten en de personen bedoeld in het derde lid in het kader van deze door hem bevolen maatregel kunnen worden gepleegd. Deze beslissing wordt in een afzonderlijk en vertrouwelijk dossier bewaard. Hij heeft als enige toegang tot dit dossier, onverminderd het in artikel 56*bis*, respectievelijk de artikelen 235*ter*, § 3 en 235*quater*, § 3 bedoelde inzagerecht van de onderzoeksrechter en de kamer van inbeschuldigingstelling. De inhoud van dit dossier valt onder het beroepsgeheim.

§ 4. De met het onderzoek belaste officier van gerechtelijke politie stelt proces-verbaal op van de verschillende fasen in de uitvoering van deze maatregel, met inbegrip van de relevante contacten. Deze processen-verbaal worden uiterlijk na het beëindigen van de maatregel bij het dossier gevoegd.

De contacten bedoeld in § 1 worden met de passende technische middelen geregistreerd en uiterlijk na het beëindigen van de maatregel bij het dossier gevoegd of ter griffie, al dan niet in digitale vorm, neergelegd.

Cette autorisation est valable pour une période de trois mois, sous réserve de renouvellement.

En cas d'urgence, l'autorisation peut être donnée verbalement. Elle doit être confirmée dans les plus brefs délais dans la forme prévue à l'alinéa précédent.

§ 3. Sont exemptés de peine, les fonctionnaires de police qui, dans le cadre de leur mission et en vue de la réussite de celle-ci ou afin de garantir leur propre sécurité ou celle d'autres personnes, commettent des infractions strictement nécessaires, ce avec l'accord exprès du procureur du Roi.

Ces infractions ne peuvent être plus graves que celles pour laquelle la mesure est utilisée et doivent nécessairement être proportionnelles à l'objectif visé.

Les alinéas 1er et 2 sont également d'application aux personnes qui ont fourni directement une aide ou une assistance nécessaire à l'exécution de cette mission ainsi qu'aux personnes visées au § 1er, alinéa 2.

Sont exemptés de peine, les magistrats qui autorisent, dans le respect du présent code, un fonctionnaire de police et la personne visée à l'alinéa 3 à commettre des infractions dans le cadre de l'exécution de la mesure.

Les fonctionnaires de police communiquent, par écrit et préalablement à l'exécution de la mesure, au procureur du Roi les infractions qu'eux-mêmes ou les personnes visées à l'alinéa 3 ont l'intention de commettre.

Si cette notification préalable n'a pas pu avoir lieu, les fonctionnaires de police informent sans délai le procureur du Roi des infractions qu'eux-mêmes ou les personnes visées à l'alinéa 3 ont commises et en donnent ensuite confirmation par écrit.

Le procureur du Roi énonce dans une décision écrite séparée les infractions pouvant être commises par les services de police et les personnes visées à l'alinéa 3 dans le cadre de la mesure ordonnée par lui. Cette décision est conservée dans un dossier séparé et confidentiel. Il est le seul à avoir accès à ce dossier, sans préjudice du droit de consultation du juge d'instruction et de la chambre des mises en accusation visé respectivement à l'article 56*bis* et aux articles 235*ter*, § 3, et 235*quater*, § 3. Le contenu de ce dossier est couvert par le secret professionnel.

§ 4. L'officier de police judiciaire chargé de l'enquête rédige le procès-verbal des différentes phases de l'exécution de cette mesure, y compris les contacts pertinents. Ces procès-verbaux sont joints au dossier au plus tard après la fin de la mesure.

Les contacts visés au § 1er sont enregistrés avec les moyens techniques appropriés et joints au dossier ou déposés au greffe, sous forme numérique ou non, au plus tard après la fin de la mesure.

De procureur des Konings of de rechter spreekt zich uit over het verzoek van de inverdenkinggestelde, de beklaagde, de burgerlijke partij of hun raadsman, om het geheel of gedeelten van de overeenkomstig het vorige lid ter griffie neergelegde geregistreerde contacten, waarvan bepaalde van belang geacht werden en overgeschreven of weergegeven werden en opgenomen werden in het proces-verbaal bedoeld in het eerste lid, te raadplegen of hiervan een kopie te ontvangen, en over hun verzoek tot overschrijving of weergave van bijkomende delen van de geregistreerde contacten

De procureur des Konings of de rechter kan het verzoek afwijzen indien hij de raadpleging, het geven van een kopie of de overschrijving of weergave van bijkomende delen niet noodzakelijk acht om de waarheid aan de dag te brengen, indien hij dit op dat ogenblik nadelig acht voor het onderzoek of om redenen die verband houden met de bescherming van andere rechten of belangen van personen. Hij kan de raadpleging, het geven van een kopie of de overschrijving of weergave van bijkomende delen ook beperken tot een door hem nader omschreven selectie van de contacten.

§ 5. De procureur des Konings staat in voor de tenuitvoerlegging van de machtigingen tot de maatregel bedoeld in § 1, eerste lid, die zijn verleend door de onderzoeksrechter in het kader van een gerechtelijk onderzoek overeenkomstig artikel 56*bis*.

De procureur des Konings vermeldt op dat ogenblik in een afzonderlijke en schriftelijke beslissing de misdrijven die door de politiediensten en de personen bedoeld § 3, derde lid, in het kader van de door de onderzoeksrechter bevolen maatregel kunnen worden gepleegd. Deze beslissing wordt in het dossier bedoeld in § 3, zevende lid, bewaard.".

Artikel 8

In artikel 47*sexies*, § 3 van hetzelfde Wetboek, ingevoegd bij wet van 6 januari 2003 en gewijzigd bij wet van 27 december 2005, worden de volgende wijzigingen aangebracht:

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

"1° de ernstige aanwijzingen van het strafbaar feit die de observatie wettigen, of, indien de observatie zich situeert in het proactieve onderzoek zoals omschreven in artikel 28*bis*, § 2, het redelijk vermoeden van te plegen of reeds gepleegde maar nog niet aan het licht gebrachte strafbare feiten, en de bijzondere aanwijzingen met betrekking tot de elementen omschreven in deze laatste bepaling, die de observatie wettigen;";

2° in de bepaling onder 5° worden de woorden "één maand" vervangen door de woorden "drie maanden".

Artikel 9

In artikel 47*octies*, § 3, van hetzelfde Wetboek, ingevoegd bij de wet van 6 januari 2003, gewijzigd door de wet van

Le procureur du Roi ou le juge se prononce sur la demande de l'inculpé, du prévenu, de la partie civile ou de leur conseil de consulter l'ensemble ou des parties des contacts enregistrés déposés au greffe conformément à l'alinéa précédent, dont certains ont été estimés pertinents et ont été retranscrits ou reproduits et consignés dans le procès-verbal visé à l'alinéa 1er, ou d'obtenir copie, ainsi que de leur demande de transcription ou de reproduction de parties supplémentaires des contacts enregistrés.

Le procureur du Roi ou le juge peut rejeter cette demande s'il estime que la consultation, la délivrance d'une copie ou la transcription ou reproduction de parties supplémentaires ne sont pas nécessaires à la manifestation de la vérité, s'il juge cette mesure, à ce moment, préjudiciable à l'enquête ou pour des raisons liées à la protection d'autres droits ou intérêts de personnes. Il peut également limiter la consultation, la délivrance d'une copie ou la transcription ou reproduction de parties supplémentaires à une sélection de contacts qu'il détermine.

§ 5. Le procureur du Roi est chargé de l'exécution des autorisations de la mesure visée au § 1er, alinéa 1er, accordées par le juge d'instruction dans le cadre d'une instruction, conformément à l'article 56*bis*.

Le procureur du Roi énonce à ce moment dans une décision écrite séparée les infractions pouvant être commises par les services de police et les personnes visées au § 3, alinéa 3, dans le cadre de la mesure ordonnée par le juge d'instruction. Cette décision est conservée dans le dossier visé au § 3, alinéa 7.".

Article 8

A l'article 47*sexies*, § 3 du même Code, inséré par la loi du 6 janvier 2003 et modifié par la loi du 27 décembre 2005, les modifications suivantes sont apportées:

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

"1° les indices sérieux de l'infraction qui justifient l'observation ou, si l'observation s'inscrit dans le cadre de l'enquête proactive définie à l'article 28*bis*, § 2, la suspicion raisonnable que des faits punissables vont être commis ou ont été commis mais ne sont pas encore connus, et les indices particuliers relatifs aux éléments décrits dans cette dernière disposition, qui justifient l'observation;";

2° au 5°, les mots "un mois" sont remplacés par les mots "trois mois".

Article 9

Dans l'article 47*octies*, § 3, du même Code, inséré par la loi de 6 janvier 2003, modifié par la loi de 27 décembre 2005 et la

27 december 2005 en de wet van 29 december 2010, wordt de bepaling onder 1° aangevuld met de woorden "of, indien de infiltratie zich situeert in het proactieve onderzoek zoals omschreven in artikel 28*bis*, § 2, het redelijk vermoeden van te plegen of reeds gepleegde maar nog niet aan het licht gebrachte strafbare feiten, en de bijzondere aanwijzingen met betrekking tot de elementen omschreven in deze laatste bepaling, die de infiltratie wettigen;".

Artikel 10

In artikel 47*undecies* van hetzelfde Wetboek, ingevoerd bij de wet van 27 december 2005 en gedeeltelijk vernietigd bij arrest nr. 105/2007 van het Grondwettelijk Hof, wordt het laatste lid opgeheven.

Artikel 11

In artikel 56*bis* van hetzelfde Wetboek, ingevoegd bij de wet van 6 januari 2003 en gewijzigd bij wet van 27 december 2005, worden de volgende wijzigingen aangebracht:

1° in lid 1 worden de woorden "of een maatregel zoals bedoeld in artikel 46*sexies*" ingevoegd tussen de woorden "bijzondere opsporingsmethoden" en de woorden "beveelt ten uitvoer gelegd";

2° lid 1 wordt aangevuld met de woorden: ", respectievelijk artikel 46*sexies*.";

3° lid 4 wordt aangevuld met de volgende zin:

"Deze personen zijn tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.".

Artikel 12

In artikel 88*bis* van hetzelfde Wetboek, ingevoegd bij de wet van 11 februari 1991 en gewijzigd bij de wetten van 30 juni 1994, 10 juni 1998, 8 juni 2008, 27 december 2012 en (dataretentiewet) worden de volgende wijzigingen aangebracht:

1° paragraaf 1 wordt vervangen als volgt:

"§ 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:

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

loi de 29 décembre 2010, le 1° est complété par les mots "ou, si l'infiltration s'inscrit dans le cadre de l'enquête proactive définie à l'article 28*bis*, § 2, la suspicion raisonnable que des faits punissables vont être commis ou ont été commis mais ne sont pas encore connus, et les indices particuliers relatifs aux éléments décrits dans cette dernière disposition, qui justifient l'infiltration;".

Article 10

Dans l'article 47*undecies* du même Code, inséré par la loi de 27 décembre 2005 et partiellement annulé par l'arrêt n° 105/2007 de la Cour constitutionnelle, le dernier alinéa est abrogé.

Article 11

A l'article 56*bis* du même code, inséré par la loi du 6 janvier 2003 et modifié par la loi du 27 décembre 2005, les modifications suivantes sont apportées:

1° dans l'alinéa 1 les mots "ou une mesure visée à l'article 46*sexies*" sont insérés entres les mots "de recherche" et les mots "sont exécutées";

2° l'alinéa 1 est complété par les mots "et 46*sexies* respectivement.";

3° l'alinéa 4 est complété par la phrase suivante:

"Ces personnes sont tenues au secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.".

Article 12

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, 27 décembre 2012 et (loi data retention), les modifications suivantes sont apportées:

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

"§ 1er. S'il existe des indices sérieux que les infractions sont de nature à entraîner un emprisonnement correctionnel principal d'un an ou 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:

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

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

Hiertoe kan hij zo nodig, rechtstreeks of via de door de Koning aangewezen politiedienst, de medewerking vorderen van:

— de operator van een elektronisch communicatienetwerk; en

— iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.

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 doet in een met redenen omkleed 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.

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 paragraaf 2.

In geval van ontdekking op heterdaad kan de procureur des Konings de maatregel bevelen voor de in artikel 90*ter*, §§ 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 347*bis*, 434 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 § 3*bis* 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° aan paragraaf 3, lid 2, wordt een zin toegevoegd, luidende:

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

Si nécessaire, il peut pour ce faire requérir, directement ou par l'intermédiaire d'un service de police désigné par le Roi, la collaboration:

— de l'opérateur d'un réseau de communications électroniques; et

— de toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.

Dans les cas visés à l'alinéa 1er, pour chaque 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, 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 également 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 paragraphe 2.

En cas de flagrant délit, le procureur du Roi peut ordonner la mesure pour les infractions visées à l'article 90*ter*, §§ 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 347*bis*, 434 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 § 3*bis* 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° paragraphe 3, alinéa 2, est complété par la phrase suivante:

"Deze personen zijn tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.".

3° in paragraaf 4 wordt lid 1 vervangen als volgt:

"De actoren bedoeld in § 1, tweede lid, delen de gegevens waarom verzocht werd mee in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, termijn waarvan de modaliteiten vastgesteld worden door de Koning, op voorstel van de minister van Justitie en de minister bevoegd voor Telecommunicatie.";

4° in paragraaf 4 wordt het derde lid vervangen als volgt:

"Iedere persoon die zijn technische medewerking aan de vorderingen bedoeld in dit artikel weigert of niet verleent in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, 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 euro tot tienduizend euro.".

Artikel 13

Artikel 88*ter* van hetzelfde Wetboek, ingevoegd bij de wet van 28 november 2000 en gewijzigd bij de wet van 6 juni 2010, wordt opgeheven.

Artikel 14

In 88*quater* van hetzelfde Wetboek, ingevoegd bij wet van 28 november 2000 en gewijzigd bij de wet van 6 juni 2010, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1 wordt het woord "personen" vervangen door de woorden "aan eenieder" en worden de woorden "of de uitbreiding ervan zoals bedoeld in artikel 39*bis*" ingevoegd tussen de woorden "het voorwerp uitmaakt van de zoeking" en de woorden "of van diensten om gegevens die worden opgeslagen";

2° paragraaf 3 wordt vervangen als volgt:

"§ 3. Hij die de in §§ 1 en 2 gevorderde medewerking niet verleent of de zoeking in het informaticasysteem of de uitbreiding ervan hindert, wordt gestraft met gevangenisstraf van zes maanden tot drie jaar en met geldboete van zesentwintig euro tot twintigduizend euro of met een van die straffen alleen.

Wanneer de medewerking bedoeld in het eerste lid de uitvoering van een misdaad of een wanbedrijf kan verhinderen, of de gevolgen ervan kan beperken, en deze medewerking niet verleend wordt, zijn de straffen een gevangenisstraf van één tot vijf jaar en een geldboete van vijfhonderd tot vijftigduizend euro.".

"Ces personnes sont tenues au secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.".

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

"Les acteurs visés au § 1er, alinéa 2, communiquent les informations demandées en temps réel ou, le cas échéant, au moment précisé dans la réquisition, délai dont les modalités sont fixées par le Roi, sur la proposition du ministre de la Justice et du ministre compétent pour les Télécommunications.";

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

"Toute personne qui refuse de prêter son concours technique aux réquisitions visées au présent article, concours dont les modalités sont fixées par le Roi, sur la proposition du ministre de la Justice et du ministre compétent pour les Télécommunications, ou ne le prête pas en temps réel ou, le cas échéant, au moment précisé dans la réquisition, est punie d'une amende de vingt-six euros à dix mille euros.".

Article 13

L'article 88*ter* du même Code, inséré par la loi du 28 novembre 2000 et modifié par la loi du 6 juin 2010, est abrogé.

Article 14

A l'article 88*quater* du même Code, inséré par la loi du 28 novembre 2000 et modifié par la loi du 6 juin 2010, les modifications suivantes sont apportées:

1° dans le paragraphe 1er les mots "aux personnes" sont remplacés par les mots "à quiconque", et les mots "ou de son extension visée à l'article 39*bis*" sont insérés entre les mots "qui fait l'objet de la recherche" et les mots "ou des services qui permettent de protéger";

2 ° le paragraphe 3 est remplacé par ce qui suit:

"§ 3. Celui qui refuse de fournir la collaboration ordonnée aux §§ 1er et 2 ou qui fait obstacle à la recherche ou à son extension dans le système informatique, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à vingt mille euros ou d'une de ces peines seulement.

Si la collaboration visée à l'alinéa 1er peut empêcher la commission d'un crime ou d'un délit ou peut en limiter les effets et que cette collaboration n'est pas fournie, les peines sont un emprisonnement de un à cinq ans et une amende de cinq cents euros à cinquante mille euros.".

Artikel 15

In artikel 89*ter* van hetzelfde Wetboek, ingevoegd bij de wet van 6 januari 2003 en gewijzigd bij de wet van 27 december 2005, wordt het eerste lid vervangen als volgt:

"In het kader van de uitvoering van de in artikel 46*quinquies* bepaalde maatregel, en onder de voorwaarden en met het oog op de doeleinden daar vermeld, kan alleen de onderzoeksrechter de politiedienst aangewezen door de Koning machtigen om:

— buiten medeweten van de eigenaar of van zijn rechthebbende, of van de bewoner, of zonder hun toestemming, te allen tijde een andere private plaats dan die welke bedoeld is artikel 46*quinquies*, § 1, te betreden, met inbegrip van het openen van gesloten voorwerpen die zich op deze plaats bevinden;

— buiten medeweten van de eigenaar, de bezitter of de gebruiker of zonder hun toestemming, zich toegang te verschaffen tot een informaticasysteem en het te doorzoeken, onverminderd de mogelijkheid voor de procureur des Konings om het binnendringen in een informaticasysteem te machtigen binnen de grenzen bepaald in artikel 46*quinquies*, § 6.".

Artikel 16

In het hetzelfde Wetboek wordt het opschrift van Boek 1, Hoofdstuk VI, Afdeling II, Onderafdeling II, paragraaf 6 vervangen als volgt:

"§ 6. Onderscheppen, kennisnemen, doorzoeken en opnemen van niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem of een deel ervan.".

Artikel 17

In artikel 90*ter* van hetzelfde Wetboek, ingevoerd bij de wet van 30 juni 1994 en laatstelijk gewijzigd bij de wet van 20 juli 2015, worden de volgende wijzigingen aangebracht:

1° paragraaf 1 wordt vervangen als volgt:

"§ 1. De onderzoeksrechter kan, onverminderd de toepassing van artikelen 39*bis*, 87, 88, 89*bis* en 90, met een heimelijk oogmerk, niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem of een deel ervan met technische hulpmiddelen onderscheppen, er kennis van nemen, doorzoeken en opnemen of de zoeking in een informaticasysteem of een deel ervan uitbreiden.

Deze maatregel kan enkel worden bevolen in uitzonderlijke gevallen, wanneer het onderzoek zulks vereist, indien er ernstige aanwijzingen bestaan dat het een strafbaar feit betreft bedoeld in een van de bepalingen opgesomd in § 2, en indien de overige middelen van onderzoek niet volstaan om de waarheid aan de dag te brengen.

Article 15

A l'article 89*ter* du même Code, inséré par la loi du 6 janvier 2003 et modifié par la loi du 27 décembre 2005, l'alinéa 1er est remplacé par ce qui suit:

"Dans le cadre de l'exécution de la mesure prévue à l'article 46*quinquies*, et aux conditions ainsi qu'aux fins qu'il énonce, seul le juge d'instruction peut autoriser le service de police d'signer par le Roi à:

— pénétrer à tout moment dans un lieu privé autre que celui visé à l'article 46*quinquies*, § 1er, en ce compris ouvrir les objets fermés se trouvant dans ce lieu, à l'insu du propriétaire ou de son ayant droit, ou de l'occupant, ou sans le consentement de ceux-ci;

— s'introduire dans un système informatique et l'explorer, à l'insu du propriétaire, du détenteur ou de l'utilisateur ou sans leur consentement, sans préjudice de la possibilité pour le procureur du Roi d'autoriser l'introduction dans un système informatique dans les limites visées à l'article 46*quinquies*, § 6.".

Article 16

Dans le même Code, l'intitulé du Livre 1, Chapitre VI, Section II, Distinction II, le paragraphe 6 est remplacé par ce qui suit:

"§ 6. Intercepter, prendre connaissance, explorer et enregistrer des communications non accessibles au public ou des données d'un système informatique ou d'une partie de celui-ci.".

Article 17

A l'article 90*ter* du même Code, inséré par la loi du 30 juin 1994 et modifié en dernier lieu par la loi du 20 juillet 2015, les modifications suivantes sont apportées:

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

"§ 1er. Sans préjudice de l'application des articles 39*bis*, 87, 88, 89*bis* et 90, le juge d'instruction peut, dans un but secret, intercepter, prendre connaissance, explorer et enregistrer, à l'aide de moyens techniques, des communications non accessibles au public ou des données d'un système informatique ou d'une partie de celui-ci, ou étendre une recherche dans un système informatique ou une partie de celui-ci.

Cette mesure ne peut être ordonnée que dans des cas exceptionnels, lorsque les nécessités de l'instruction l'exigent, s'il existe des indices sérieux que cela concerne une infraction visée par l'une des dispositions énumérées au § 2, et si les autres moyens d'investigation ne suffisent pas à la manifestation de la vérité.

Teneinde deze maatregel mogelijk te maken, kan de onderzoeksrechter bevelen om, te allen tijde, ook buiten medeweten of zonder de toestemming van hetzij de bewoner, hetzij de eigenaar of zijn rechthebbende, hetzij de gebruiker:

— in een woning, in een private plaats of in een informaticasysteem binnen te dringen;

— elke beveiliging van de betrokken informaticasystemen tijdelijk op te heffen, desgevallend met behulp van technische hulpmiddelen, valse signalen, valse sleutels of valse hoedanigheden;

— technische middelen in de betrokken informaticasystemen aan te brengen teneinde de door dat systeem opgeslagen, verwerkte of doorgestuurde gegevens te ontcijferen en te decoderen.

De maatregel bedoeld in deze paragraaf kan alleen worden bevolen om de gegevens op te sporen die kunnen dienen om de waarheid aan de dag te brengen. Hij kan alleen worden bevolen ten aanzien van personen die op grond van precieze aanwijzingen ervan verdacht worden het strafbare feit te hebben gepleegd, ten aanzien van de communicatiemiddelen of informaticasystemen die geregeld worden gebruikt door een persoon op wie een verdenking rust of ten aanzien van de plaatsen waar deze vermoed wordt te vertoeven. De maatregel kan eveneens worden bevolen ten aanzien van personen van wie op grond van precieze feiten vermoed wordt dat zij geregeld in verbinding staan met een persoon op wie een verdenking rust.";

2° paragraaf 2 wordt vervangen als volgt:

"§ 2. De strafbare feiten die de maatregel bedoeld in § 1 kunnen wettigen zijn degene die bedoeld worden in:

1° de artikelen 101 tot en met 110 van het Strafwetboek;

2° De artikelen 136*bis*, 136*ter*, 136*quater*, 136*sexies* en 136*septies* van hetzelfde Wetboek en artikel 41 van de wet van 29 maart 2004 betreffende de samenwerking met het Internationaal Strafgerechtshof en de internationale straftribunalen;

3° Boek II, Titel I*ter*, van hetzelfde Wetboek;

4° artikel 147 van hetzelfde Wetboek;

5° de artikelen 160, 161, 162, 163, 168, 171, 173 en 176 van hetzelfde Wetboek;

6° de artikelen 180 en 186 van hetzelfde Wetboek;

7° artikel 210*bis* van hetzelfde Wetboek;

8° de artikelen 246, 247, 248, 249, en 250 van hetzelfde Wetboek;

9° artikel 259*bis* van hetzelfde Wetboek;

10° artikel 314*bis* van hetzelfde Wetboek;

En vue de permettre cette mesure, le juge d'instruction peut également, à l'insu ou sans le consentement de l'occupant, du propriétaire ou de son ayant droit, ou de l'utilisateur, ordonner, à tout moment:

— la pénétration dans un domicile, un lieu privé ou un système informatique;

— la suppression temporaire de toute protection des systèmes informatiques concernés, le cas échéant à l'aide de moyens techniques, de faux signaux, de fausses clés ou de fausses qualités;

— l'installation de dispositifs techniques dans les systèmes informatiques concernés en vue du décryptage et du décodage de données stockées, traitées ou transmises par ce système.

La mesure visée dans ce paragraphe peut uniquement être ordonnée pour rechercher les données qui peuvent servir à la manifestation de la vérité. Elle ne peut être ordonnée qu'à l'égard soit de personnes soupçonnées, sur la base d'indices précis, d'avoir commis l'infraction, soit à l'égard des moyens de communication ou systèmes informatiques régulièrement utilisés par un suspect, soit à l'égard des lieux présumés fréquentés par celui-ci. Elle peut également être ordonnée à l'égard de personnes présumées, sur la base de faits précis, être en communication régulière avec un suspect.";

2° le paragraphe 2 est remplacé par ce qui suit:

"§ 2. Les infractions pouvant justifier la mesure visée au § 1er sont celles qui sont visées:

1° aux articles 101 à 110 du Code pénal;

2° aux articles 136*bis*, 136*ter*, 136*quater*, 136*sexies* et 136*septies* du même Code et à l'article 41 de la loi du 29 mars 2004 concernant la coopération avec la Cour pénale internationale et les tribunaux pénaux internationaux;

3° au livre II, titre I*ter*, du même Code;

4° à l'article 147 du même Code;

5° aux articles 160, 161, 162, 163, 168, 171, 173 et 176 du même Code;

6° aux articles 180 et 186 du même Code;

7° à l'article 210*bis* du même Code;

8° aux articles 246, 247, 248, 249 et 250 du même Code;

9° à l'article 259*bis* du même Code;

10° à l'article 314*bis* du même Code;

11° de artikelen 324*bis* en 324*ter* van hetzelfde Wetboek;

12° de artikelen 327, 328, 329 of 330 van hetzelfde Wetboek, voor zover een klacht is ingediend;

13° artikel 331*bis* van hetzelfde Wetboek;

14° artikel 347*bis* van hetzelfde Wetboek;

15° de artikelen 372 tot 377*bis* van hetzelfde Wetboek;

16° artikel 377*quater* van hetzelfde Wetboek;

17° de artikelen 379, 380 en 383*bis*, § 1 en 3 van hetzelfde Wetboek;

18° artikel 393 van hetzelfde Wetboek;

19° de artikelen 394 of 397 van hetzelfde Wetboek;

20° de artikelen 428 en 429 van hetzelfde Wetboek;

21° artikel 433*bis*/1 van hetzelfde Wetboek;

22° de artikelen 433*quinquies* tot 433*octies* van hetzelfde Wetboek;

23° artikel 434 van hetzelfde Wetboek;

24° de artikelen 468, 470, 471 of 472 van hetzelfde Wetboek;

25° artikel 475 van hetzelfde Wetboek;

26° boek II, titel IX, hoofdstuk I, sectie 2*bis*, en hoofdstuk I*bis* van hetzelfde Wetboek;

27° de artikelen 504*bis* en 504*ter* van hetzelfde Wetboek;

28° artikel 504*quater* van hetzelfde Wetboek;

29° artikel 505, eerste lid, 1° van hetzelfde Wetboek wanneer de betrokken zaken werden weggenomen, verduisterd of verkregen door een misdaad of wanbedrijf vermeld in dit artikel;

29*bis*° artikel 505, eerste lid, 2°, 3° en 4° van hetzelfde Wetboek;

30° de artikelen 510, 511, eerste lid of 516 van hetzelfde Wetboek;

31° artikel 520 van hetzelfde Wetboek, indien de omstandigheden bedoeld in de artikelen 510 of 511, eerste lid, van hetzelfde Wetboek verenigd zijn;

32° artikelen 550*bis* en 550*ter* van hetzelfde Wetboek;

33° artikel 2*bis* van de wet van 24 februari 1921 betreffende het verhandelen van giftstoffen, slaapmiddelen en verdovende middelen, psychotrope stoffen, ontsmettingsstoffen

11° aux articles 324*bis* et 324*ter* du même Code;

12° aux articles 327, 328, 329 ou 330 du même Code, pour autant qu'une plainte ait été déposée;

13° à l'article 331*bis* du même Code;

14° à l'article 347*bis* du même Code;

15° aux articles 372 à 377*bis* du même Code;

16° à l'article 377*quater* du même Code;

17° aux articles 379, 380 et 383*bis*, §§ 1er et 3, du même Code;

18° à l'article 393 du même Code;

19° aux articles 394 ou 397 du même Code;

20° aux articles 428 et 429 du même Code;

21° à l'article 433*bis*/1 du même Code;

22° aux articles 433*quinquies* à 433*octies* du même Code;

23° à l'article 434 du même Code;

24° aux articles 468, 470, 471 ou 472 du même Code;

25° à l'article 475 du même Code;

26° au livre II, titre IX, chapitre Ier, section 2*bis*, et chapitre Ier*bis* du même Code;

27° aux articles 504*bis* et 504*ter* du même Code;

28° à l'article 504*quater* du même Code;

29° à l'article 505, alinéa 1er, 1° du même Code lorsque les choses concernées ont été enlevées, détournées ou obtenues à l'aide d'un crime ou d'un délit visés au présent article;

29*bis*° à l'article 505, alinéa premier, 2°, 3° et 4° du même Code;

30° aux articles 510, 511, alinéa 1er, ou 516 du même Code;

31° à l'article 520 du même Code, si les circonstances visées aux articles 510 ou 511, alinéa 1er, du même Code sont réunies;

32° aux articles 550*bis* et 550*ter* du même Code;

33° à l'article 2*bis* de la loi du 24 février 1921 concernant le trafic des substances vénéneuses, soporifiques, stupéfiantes, psychotropes, désinfectantes ou antiseptiques et

en antiseptica en van de stoffen die kunnen gebruikt worden voor de illegale vervaardiging van verdovende middelen en psychotrope stoffen;

34° artikel 145, § 3 en § 3*bis* van de wet van 13 juni 2005 betreffende de elektronische communicatie;

35° artikel 10 van de wet van 5 augustus 1991 betreffende de in-, uit- en doorvoer van wapens, munitie en speciaal voor militair gebruik dienstig materieel en daaraan verbonden technologie;

36° artikel 47 van het decreet van het Vlaams Parlement van 15 juni 2012 betreffende de in-, uit-, doorvoer en overbrenging van defensiegerelateerde producten, ander voor militair gebruik dienstig materiaal, ordehandhavingsmateriaal, civiele vuurwapens, onderdelen en munitie;

37° artikel 20 van het decreet van het Waals Gewest van 21 juni 2012 betreffende de invoer, uitvoer, doorvoer en overdracht van civiele wapens en van defensiegerelateerde producten;

38° artikel 42 van de ordonnantie van het Brussels Hoofdstedelijk gewest van 20 juni 2013 betreffende de in-, uit-, doorvoer en overbrenging van defensiegerelateerde producten, ander voor militair gebruik dienstig materiaal, ordehandhavingsmateriaal, civiele vuurwapens, onderdelen, toebehoren en munitie ervan;

39° artikelen 8 tot 11, 14, 16, 19, 1°, 2°, 3°, 5° en 6°, 20, 22, 27 en 33 van de wet van 8 juni 2006 houdende regeling van economische en individuele activiteiten met wapens, ook "wapenwet" genoemd;

40° de wet van 28 mei 1956 betreffende ontplofbare en voor de deflagratie vatbare stoffen en mengsels en de daarmede geladen tuigen;

41° artikelen 21 tot 26 van het Samenwerkingsakkoord tussen de Federale Staat, het Vlaams Gewest, het Waals Gewest en het Brussels Hoofdstedelijk Gewest betreffende de uitvoering van de overeenkomst tot verbod van de ontwikkeling, de productie, de aanleg van voorraden en het gebruik van chemische wapens en inzake de vernietiging van deze wapens, gedaan te Parijs op 13 januari 1993;

42° de artikelen 77*bis* tot 77*quinquies* van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen;

43° artikel 10, § 1, 2°, van de wet van 15 juli 1985 betreffende het gebruik bij dieren van stoffen met hormonale, anti-hormonale, beta-adrenergische of productie-stimulerende werking;

44° artikel 1 van het koninklijk besluit van 12 april 1974 betreffende sommige verrichtingen in verband met stoffen met hormonale, anti-hormonale, anabole, anti-infectieuze, anti-parasitaire, en anti-inflammatoire werking, welk artikel betrekking heeft op strafbare feiten waarop overeenkomstig

des substances pouvant servir à la fabrication illicite de substances stupéfiantes et psychotropes;

34° à l'article 145, §§ 3 et 3*bis*, de la loi du 13 juin 2005 relative aux communications électroniques;

35° à l'article 10 de la loi du 5 août 1991 relative à l'importation, à l'exportation et au transit d'armes, de munitions et de matériel devant servir spécialement à un usage militaire et de la technologie y afférente;

36° à l'article 47 du décret du parlement flamand du 15 juin 2012 concernant l'importation, l'exportation, le transit et le transfert de produits liés à la défense, d'autre matériel à usage militaire, de matériel de maintien de l'ordre, d'armes à feu civiles, de pièces et de munitions;

37° à l'article 20 du décret de la Région wallonne du 21 juin 2012 relatif à l'importation, à l'exportation, au transit et au transfert d'armes civiles et de produits liés à la défense;

38° à l'article 42 de l'ordonnance de la Région de Bruxelles-Capitale du 20 juin 2013 relative à l'importation, à l'exportation, au transit et au transfert de produits liés à la défense, d'autre matériel pouvant servir à un usage militaire, de matériel lié au maintien de l'ordre, d'armes à feu à usage civil, de leurs pièces, accessoires et munitions;

39° aux articles 8 à 11, 14, 16, 19, 1°, 2°, 3°, 5° et 6°, 20, 22, 27 et 33 de la loi du 8 juin 2006 réglant des activités économiques et individuelles avec des armes, aussi appelée "Loi sur les armes";

40° à la loi du 28 mai 1956 relative aux substances et mélanges explosibles ou susceptibles de déflagrer et aux engins qui en sont chargés;

41° aux articles 21 à 26 de l'Accord de Coopération du 2 mars 2007 entre l'État fédéral, la Région flamande, la Région wallonne et la Région de Bruxelles-Capitale relatif à l'exécution de la Convention sur l'interdiction de la mise au point, de la fabrication, du stockage et de l'emploi des armes chimiques et sur leur destruction, faite à Paris le 13 janvier 1993;

42° aux articles 77*bis* à 77*quinquies* de la loi du 15 décembre 1980 concernant l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers;

43° à l'article 10, § 1er, 2°, de la loi du 15 juillet 1985 relative à l'utilisation de substances à effet hormonal, à effet antihormonal, à effet bêta-adrénergique ou à effet stimulateur de production chez les animaux;

44° article 1er de l'arrêté royal du 12 avril 1974 relatif à certaines opérations concernant les substances à action hormonale, antihormonale, anabolisante, bêta-adrénergique, anti-infectieuse, antiparasitaire et anti-inflammatoire, article précité visant des infractions punies conformément à la

de wet van 24 februari 1921 betreffende het verhandelen van de gifstoffen, slaapmiddelen en verdovende middelen, ontsmettingsstoffen en antiseptica straffen worden gesteld.";

3° in de paragrafen 3 en 4 wordt het woord "bewakingsmaatregel" telkens vervangen door het woord "maatregel";

4° paragraaf 5 wordt vervangen als volgt:

"§ 5. Ingeval van ontdekking op heterdaad en zolang de heterdaadsituatie duurt, kan de procureur des Konings de maatregel bedoeld in § 1 bevelen voor de strafbare feiten bedoeld in de artikelen 347*bis*, 434, of 470 van het Strafwetboek.";

5° in paragraaf 6, eerste lid, worden de woorden "tijdelijk privételecommunicatie afluisteren, er kennis van nemen en opnemen tijdens de overbrenging ervan" vervangen door de woorden "tijdelijk niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem onderscheppen, er kennis van nemen en opnemen".

Artikel 18

Artikel 90*quater* van hetzelfde Wetboek, ingevoegd bij de wet van 30 juni 1994 en laatstelijk gewijzigd bij de wet van 5 februari 2016, wordt vervangen als volgt:

"Art. 90*quater*. § 1. Tot iedere maatregel op grond van artikel 90*ter* verleent de onderzoeksrechter een schriftelijke voorafgaande met redenen omklede machtiging die hij meedeelt aan de procureur des Konings.

De machtiging wordt gedagtekend en vermeldt:

1° de aanwijzingen en de concrete feiten, eigen aan de zaak, die de maatregel wettigen overeenkomstig artikel 90*ter*;

2° de redenen waarom de maatregel onontbeerlijk is om de waarheid aan de dag te brengen;

3° de persoon, het communicatiemiddel, het informaticasysteem of de plaats die het voorwerp is van de bewaking;

4° de periode tijdens dewelke de maatregel kan worden uitgeoefend, die niet langer mag zijn dan één maand. Deze termijn vangt aan de dag van de machtiging waarbij de maatregel wordt bevolen, of, ingeval van artikel 90*quinquies*, eerste lid, verlengd, en loopt tot en met de dag voor de zoveelste van de daarop volgende maand;

5° de naam en de hoedanigheid van de officier of officieren van gerechtelijke politie aangewezen voor de uitvoering van de maatregel.

In spoedeisende gevallen kan de machtiging mondeling worden verleend. Deze machtiging moet uiterlijk binnen vierentwintig uren worden bevestigd in de vorm bepaald in het tweede lid.

§ 2. De onderzoeksrechter kan, om de maatregel bedoeld in artikel 90*ter*, § 1, mogelijk te maken, rechtstreeks of via

loi du 24 février 1921 concernant le trafic des substances vénéneuses, soporifiques, stupéfiantes, désinfectantes ou antiseptiques.";

3° aux paragraphes 3 et 4 les mots "mesures de surveillance" sont chaque fois remplacés par le mot "mesure";

4° le paragraphe 5 est remplacé par ce qui suit:

"§ 5. En cas de flagrant délit et tant que la situation de flagrant délit perdure, le procureur du Roi peut ordonner la mesure visée au § 1er pour les infractions visées aux articles 347*bis*, 434 ou 470 du Code pénal.";

5° au paragraphe 6, alinéa 1er, les mots "temporairement écouter, prendre connaissance et enregistrer, pendant leur transmission, des télécommunications privées" sont remplacés par les mots "intercepter, prendre connaissance et enregistrer des communications non accessibles au public ou des données d'un système informatique".

Article 18

L'article 90*quater* du même Code, inséré par la loi du 30 juin 1994 et modifié en dernier lieu par la loi du 5 février 2016, est remplacé par ce qui suit:

"Art. 90*quater*. § 1er. Toute mesure sur la base de l'article 90*ter* fait l'objet d'une autorisation écrite préalable et motivée du juge d'instruction, que celui-ci communique au procureur du Roi.

L'autorisation est datée et indique:

1° les indices ainsi que les faits concrets et propres à la cause qui justifient la mesure conformément à l'article 90*ter*;

2° les motifs pour lesquels la mesure est indispensable à la manifestation de la vérité;

3° la personne, le moyen de communication, le système informatique ou le lieu soumis à la surveillance;

4° la période pendant laquelle la mesure peut être exécutée et qui ne peut excéder un mois. Ce délai commence à courir le jour de l'autorisation ordonnant ou, dans le cas de l'article 90*quinquies*, alinéa 1er, prolongeant la mesure et s'achève la veille du quantième du mois suivant;

5° les nom et qualité de l'officier ou des officiers de police judiciaire commis pour l'exécution de la mesure.

En cas d'urgence, l'autorisation peut être donnée verbalement. Elle doit être confirmée dans la forme prévue à l'alinéa 2 au plus tard dans les vingt-quatre heures.

§ 2. Afin de permettre la mesure visée à l'article 90*ter*, § 1er, le juge d'instruction peut requérir, directement ou par

de tussenkomst van een politiedienst aangewezen door de Koning, de medewerking vorderen van:

— de operator van een elektronisch communicatienetwerk, en

— iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.

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 aan de vorderingen bedoeld in de vorige leden weigert of niet verleent in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, 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 euro tot twintigduizend euro.

§ 3. De onderzoeksrechter mag voor de tenuitvoerlegging van de maatregel bedoeld in artikel 90*ter*, § 1 alleen officieren van gerechtelijke politie aanwijzen. Deze kunnen zich echter laten bijstaan door agenten van gerechtelijke politie en, onder de voorwaarden door de Koning bepaald, door personeelsleden van het administratief en logistiek kader van de geïntegreerde politie. De laatstgenoemde personen mogen niet belast worden met de analyse van de inhoud van de opgenomen communicatie of gegevens, tenzij het een specifieke expertise betreft, of met de selectie van voor het onderzoek relevant geachte delen, zoals bedoeld in artikel 90*sexies*, § 1, 2°.

De officieren van gerechtelijke politie houden de namen bij van de personen door wie zij zich laten bijstaan, in een lijst die voor elk dossier afzonderlijk wordt opgesteld volgens de modaliteiten door de Koning bepaald, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer. Indien deze personen belast zijn met de uitvoering van het bevel bedoeld in artikel 90*ter*, § 1, derde lid, worden hun namen niet vermeld in het gerechtelijk dossier.

De aangewezen officieren van gerechtelijke politie brengen ten minste om de vijf dagen schriftelijk verslag uit aan de onderzoeksrechter over de tenuitvoerlegging van de beschikking.

§ 4. De onderzoeksrechter kan personen waarvan hij vermoedt dat ze een bijzondere kennis hebben van het communicatiemiddel of het informaticasysteem waarop de maatregel betrekking heeft of van diensten of toepassingen om gegevens, die worden opgeslagen, verwerkt of overgedragen via een communicatiemiddel of een informaticasysteem, te

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

— de l'opérateur d'un réseau de communications électroniques; et

— de toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.

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 aux alinéas précédents, concours dont les modalités sont fixées par le Roi, sur la proposition du ministre de la Justice et du ministre compétent pour les Télécommunications, ou ne le prête pas en temps réel ou, le cas échéant, au moment précisé dans la réquisition, est punie d'une amende de vingt-six euros à vingt mille euros.

§ 3. Le juge d'instruction ne peut commettre pour l'exécution de la mesure visée à l'article 90*ter*, § 1er, que des officiers de police judiciaire. Ceux-ci peuvent néanmoins se faire assister par des agents de police judiciaire et, selon les conditions fixées par le Roi, par des agents du cadre administratif et logistique de la police intégrée. Ces dernières personnes ne peuvent être chargées de l'analyse du contenu des communications ou données enregistrées, sauf s'il s'agit d'une expertise spécifique, ou de la sélection des parties estimées pertinentes pour l'instruction, comme prévu à l'article 90*sexies*, § 1er, 2°.

Les officiers de police judiciaire conservent les noms des personnes qui peuvent les assister dans une liste établie séparément pour chaque dossier selon les modalités fixées par le Roi, après avis de la Commission pour la protection de la vie privée. Si ces personnes sont chargées de l'exécution de l'ordonnance visée à l'article 90*ter*, § 1er, alinéa 3, leur nom n'est pas mentionné dans le dossier judiciaire.

Les officiers de police judiciaire commis font rapport par écrit au moins tous les cinq jours au juge d'instruction sur l'exécution de l'ordonnance.

§ 4. Le juge d'instruction peut exiger, directement ou par le l'intermédiaire d'un service de police désigné par le Roi, de personnes dont il présume qu'elles ont une connaissance particulière du moyen de communication ou du système informatique qui fait l'objet de la mesure ou de services ou applications qui permettent de protéger, de coder ou de

beveiligen, te coderen of te versleutelen, rechtstreeks of via de tussenkomst van een politiedienst aangewezen door de Koning, vorderen inlichtingen te verlenen over de werking ervan en over de wijze om in een verstaanbare vorm toegang te verkrijgen tot de inhoud ervan die wordt of is overgebracht.

Hij kan personen vorderen om deze inhoud toegankelijk te maken in de door hem gewenste vorm.

Iedere persoon die zijn technische medewerking weigert aan de vorderingen bedoeld in de vorige leden, wordt gestraft met gevangenisstraf van zes maanden tot een jaar en met geldboete van zesentwintig euro tot twintigduizend euro of met een van die straffen alleen.

Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of gevorderd wordt zijn technische medewerking te verlenen, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

§ 5. In voorkomend geval is artikel 39*bis*, § 4, vierde lid toepasbaar op de gegevens, aangetroffen door een zoeking in een informaticasysteem met toepassing van artikel 90*ter*, § 1.".

Artikel 19

In artikel 90*quinquies* van hetzelfde Wetboek, ingevoegd bij de wet van 30 juni 1994, worden de volgende wijzigingen aangebracht:

1° het eerste lid wordt vervangen als volgt:

"De onderzoeksrechter kan de uitwerking van de machtiging bedoeld in artikel 90*quater*, § 1, één of meer malen verlengen met een termijn die niet langer mag zijn dan één maand, met een maximum van zes maanden, onverminderd zijn beslissing om aan de maatregel een einde te maken zodra de omstandigheden die deze gewettigd hebben, verdwenen zijn. Deze termijn van zes maanden vangt aan de dag van de eerste machtiging waarbij de maatregel wordt bevolen, en loopt tot en met de dag voor de zoveelste van de zesde daarop volgende maand. Indien de maatregel, wegens de technische voorbereiding ervan, daadwerkelijk werd aangevat op een latere dag dan deze van de eerste machtiging, vangt de termijn van zes maanden aan de dag van deze daadwerkelijke aanvatting en ten laatste twee maanden na de dag van de eerste machtiging.";

2° in het tweede en het derde lid wordt het woord "beschikking" telkens vervangen door het woord "machtiging".

Artikel 20

Artikel 90*sexies* van hetzelfde Wetboek, ingevoegd bij de wet van 30 juni 1994 en gewijzigd bij de wetten van 10 juni 1998 en 5 februari 2016, wordt vervangen als volgt:

"§ 1. De aangewezen officieren van gerechtelijke politie stellen aan de onderzoeksrechter ter beschikking:

crypter les données qui sont stockées, traitées ou transmises par un moyen de communication ou un système informatique, qu'elles fournissent des informations sur le fonctionnement de ce moyen ou système et sur la manière d'accéder à son contenu qui est ou a été transmis, dans une forme compréhensible.

Il peut ordonner aux personnes de rendre accessible ce contenu, dans la forme qu'il aura souhaitée.

Toute personne qui refuse de prêter son concours technique aux réquisitions visées aux alinéas précédents est punie d'un emprisonnement de six mois à un an et d'une amende de vingt-six euros à vingt mille euros ou d'une de ces peines seulement.

Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou est requise d'y prêter son concours technique, est tenue au secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

§ 5. Le cas échéant, l'article 39*bis*, § 4, alinéa 4, est applicable aux données recueillies par une recherche dans un système informatique en application de l'article 90*ter*, § 1er.".

Article 19

A l'article 90*quinquies* du même Code, inséré par la loi du 30 juin 1994, les modifications suivantes sont apportées:

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

"Le juge d'instruction peut prolonger une ou plusieurs fois les effets de son autorisation visée à l'article 90*quater*, § 1er, pour un nouveau terme qui ne peut dépasser un mois, avec un maximum de six mois, sans préjudice de sa décision de mettre fin à la mesure dès que les circonstances qui l'ont justifiée ont disparu. Ce délai de six mois commence à courir le jour de la première autorisation ordonnant la mesure et s'achève la veille du quantième du sixième mois suivant. Si la mesure, en raison de sa préparation technique, a effectivement débuté un jour postérieur à celui de la première autorisation, ce délai de six mois commence à courir au moment de ce début effectif et au plus tard deux mois après le jour de la première autorisation.";

2° dans les alinéas 2 et 3, le mot "ordonnance" est chaque fois remplacé par le mot "autorisation".

Article 20

L'article 90*sexies* du même Code, inséré par la loi du 30 juin 1994 et modifié par les lois du 10 juin 1998 et 5 février 2016, est remplacé par ce qui suit:

"§ 1er. Les officiers de police judiciaire commis mettent à la disposition du juge d'instruction:

1° Het bestand bevattende de opgenomen niet voor publiek toegankelijke communicaties of gegevens van een informaticasysteem bekomen als gevolg van de maatregelen genomen met toepassing van de artikelen 90*ter*, 90*quater* en 90*quinquies*;

2° De overschrijving of weergave van de door de aangewezen officieren van gerechtelijke politie voor het onderzoek van belang geachte gedeelten van de opgenomen communicaties of gegevens, en de eventuele vertaling ervan;

3° In voorkomend geval, de plaats van de gegevens, bedoeld in 2°, in het informaticasysteem;

4° Een algemene beschrijving van de inhoud en van de identificatiegegevens van de gebruikte communicatiemiddelen of informaticasystemen wat betreft de niet van belang geachte communicaties of gegevens.

§ 2. Onverminderd de selectie door de officieren van gerechtelijke politie bedoeld in § 1, beoordeelt de onderzoeksrechter welke gedeelten van alle opgenomen niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem van belang zijn voor het onderzoek. In zoverre deze gedeelten van de communicatie of gegevens niet overgeschreven, weergegeven of vertaald zijn overeenkomstig § 1, moeten zij bijkomend overgeschreven, weergegeven en eventueel vertaald worden. De onderzoeksrechter laat daarvan proces-verbaal opmaken.

§ 3. De niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem die onder het beroepsgeheim vallen, worden niet opgetekend in het proces-verbaal. Deze communicatie of gegevens worden in een bestand onder verzegelde omslag neergelegd ter griffie. Gaat het om personen bedoeld in artikel 90*octies*, dan wordt ter zake gehandeld zoals bepaald in dat artikel.

§ 4. De machtigingen van de onderzoeksrechter, de verslagen van de officieren van gerechtelijke politie bedoeld in artikel 90*quater*, § 3, en de processen-verbaal die betrekking hebben op de tenuitvoerlegging van de maatregel, worden uiterlijk na het beëindigen van de maatregelen bij het dossier gevoegd.”.

Artikel 21

Artikel 90*septies* van hetzelfde Wetboek, ingevoegd bij de wet van 30 juni 1994 en gewijzigd bij de wetten van 10 juni 1998, 28 november 2000 en 5 februari 2016, wordt vervangen als volgt:

“Art. 90*septies*. § 1. De passende middelen worden aangewend om de integriteit en de vertrouwelijkheid van de opgenomen niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem te waarborgen.

§ 2. Ieder bestand bevat het onderwerp van de opgenomen niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem en de dagen en uren waarop de maatregel is uitgevoerd.

1° le fichier contenant les communications non accessibles au public ou les données d’un système informatique enregistrées et obtenues à la suite des mesures prises en application des articles 90*ter*, 90*quater* et 90*quinquies*;

2° la transcription ou reproduction des parties des communications ou données enregistrées estimées pertinentes pour l’instruction par les officiers de police judiciaire commis, et leur traduction éventuelle;

3° le cas échéant, l’endroit où se trouvent les données visées au 2° dans le système informatique;

4° Une description générale du contenu et des données d’identification des moyens de communication ou systèmes informatiques utilisés en ce qui concerne les communications ou données estimées non pertinentes.

§ 2. Sans préjudice de la sélection par les officiers de police judiciaire visés au § 1er, le juge d’instruction apprécie parmi toutes les communications non accessibles au public ou données d’un système informatique qui ont été enregistrées les parties qui sont pertinentes pour l’instruction. Dans la mesure où ces parties de communications ou données n’ont pas été transcrites, reproduites ou traduites conformément au § 1er, elles seront transcrites, reproduites et éventuellement traduites. Le juge d’instruction en fait dresser procès-verbal.

§ 3. Les communications non accessibles au public ou données d’un système informatique qui sont couvertes par le secret professionnel ne sont pas consignées dans le procès-verbal. Ces communications ou données sont déposées au greffe dans un fichier sous pli scellé. S’il s’agit de personnes visées à l’article 90*octies*, on procède ainsi qu’il est prévu à cet article.

§ 4. Les autorisations du juge d’instruction, les rapports des officiers de police judiciaire visés à l’article 90*quater*, § 3, et les procès-verbaux relatifs à l’exécution de la mesure, sont joints au dossier au plus tard après qu’il est mis fin à la mesure.”.

Article 21

L’article 90*septies* du même Code, inséré par la loi du 30 juin 1994 et modifié par les lois du 10 juin 1998, 28 novembre 2000 et 5 février 2016, est remplacé par ce qui suit:

“Art. 90*septies*. § 1er. Les moyens appropriés sont utilisés pour garantir l’intégrité et la confidentialité des communications non accessibles au public ou données d’un système informatique qui ont été enregistrées.

§ 2. Chaque fichier contient le sujet des communications non accessibles au public ou données d’un système informatique qui ont été enregistrées ainsi que les jours et heures auxquels la mesure a été exécutée.

§ 3. Iedere aantekening in het kader van de tenuitvoerlegging van de maatregelen bedoeld in de artikelen 90*ter*, 90*quater* en 90*quinquies* door de daartoe aangewezen personen, die niet is opgetekend in een proces-verbaal, wordt vernietigd, met uitzondering van het vermelde in artikel 90*sexies*, § 1, 2°, 3° en 4° en onverminderd artikel 33 van de wet van … betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecommunicaties. De voor de uitvoering van de maatregel aangewezen officieren van gerechtelijke politie gaan over tot deze vernietiging en vermelden dit in een proces-verbaal.

Om beheersredenen en om aan de verplichting van artikel 90*decies* te kunnen voldoen, kunnen de strikt noodzakelijke administratieve gegevens evenwel bewaard blijven bij de dienst aangewezen door de Koning.

§ 4. De bestanden bedoeld in artikel 90*sexies*, § 1, 1° worden bewaard onder verzegelde omslag ter griffie. Ze kunnen bovendien ook worden bewaard bij de dienst aangewezen door de Koning onder de voorwaarden en modaliteiten door Hem bepaald na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer.

De stukken bedoeld in artikel 90*sexies*, § 1, 2°, 3° en 4° en de afschriften van de processen-verbaal worden onder verzegelde omslag ter griffie bewaard.

§ 5. De griffier vermeldt in een per dag bijgehouden, bijzonder register:

1° de dag van de neerlegging van de in artikel 90*sexies*, § 1 bedoelde bestanden en stukken, alsmede van ieder afschrift van proces-verbaal;

2° de naam van de onderzoeksrechter die de maatregelen heeft bevolen of bevestigd en het voorwerp ervan;

3° de dag waarop de zegels zijn verbroken en in voorkomend geval opnieuw zijn gelegd;

4° de datum van de kennisname van de in artikel 90*sexies*, § 1 bedoelde bestanden en stukken, van de afschriften van processen-verbaal, alsook de namen van de personen er kennis van genomen hebben.

Ingeval de kennisname een bestand betreft dat wordt bewaard bij de federale politie, overeenkomstig § 4, eerste lid, wordt het daartoe tijdelijk ter beschikking gesteld ter griffie, uiterlijk tot na de kennisname ervan;

5° iedere andere gebeurtenis die erop betrekking heeft.

§ 6. De inverdenkinggestelde, de beklaagde, de burgerlijke partij of hun raadsman ontvangen op eenvoudig verzoek een kopie van het geheel van de opgenomen niet voor het publiek toegankelijke communicaties of gegevens van een informaticasysteem, waarvan bepaalde van belang geachte gedeelten overgeschreven of weergegeven werden en opgenomen werden in een proces-verbaal waarvan ze inzage hebben.

§ 3. Toute note prise dans le cadre de l'exécution des mesures visées aux articles 90*ter*, 90*quater* et 90*quinquies* par les personnes commises à cette fin qui n'est pas consignée dans un procès-verbal, est détruite, à l'exception de ce qui est mentionné à l'article 90*sexies*, § 1er, 2°, 3° et 4°, et sans préjudice de l'article 33 de la loi du … relative à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications. Les officiers de police judiciaire commis pour l'exécution de la mesure procèdent à cette destruction et en font mention dans un procès-verbal.

Pour des raisons de gestion et en vue du respect de l'obligation de l'article 90*decies*, les données administratives strictement nécessaires peuvent néanmoins être conservées au sein du service désigné par le Roi.

§ 4. Les fichiers visés à l'article 90*sexies*, § 1er, 1°, sont conservés au greffe sous pli scellé. Ils peuvent en outre être conservés au sein du service désigné par le Roi aux conditions et modalités fixées par Lui après avis de la Commission de la protection de la vie privée.

Les pièces visées à l'article 90*sexies*, § 1er, 2°, 3° et 4°, et les copies des procès-verbaux sont conservées au greffe sous pli scellé.

§ 5. Le greffier mentionne dans un registre spécial tenu journellement:

1° le jour du dépôt des fichiers et pièces visés à l'article 90*sexies*, § 1er, ainsi que de chaque copie de procès-verbal;

2° le nom du juge d'instruction qui a ordonné ou confirmé la mesure et l'objet de celle-ci;

3° le jour où les scellés sont ouverts et éventuellement réapposés;

4° la date de prise de connaissance des fichiers et pièces visés à l'article 90*sexies*, § 1er, des copies des procès-verbaux, ainsi que le nom des personnes qui en ont pris connaissance.

Si la prise de connaissance concerne un fichier conservé à la police fédérale, conformément au § 4, alinéa 1er, le fichier est mis temporairement à disposition au greffe à cette fin, au plus tard jusqu'après la prise de connaissance;

5° tous les autres événements qui s'y rapportent.

§ 6. L'inculpé, le prévenu, la partie civile ou leurs conseils reçoivent, sur simple demande, copie de la totalité des communications non accessibles au public ou données d'un système informatique, dont certaines parties estimées pertinentes ont été transcrites ou reproduites et consignées dans un procès-verbal qu'ils ont le droit de consulter.

De inverdenkinggestelde, de beklaagde, de burgerlijke partij of hun raadsman kunnen de rechter verzoeken om de overeenkomstig § 4 ter griffie of bij de dienst aangewezen door de Koning neergelegde andere bestanden of stukken ter griffie te raadplegen, en bijkomende delen van de opgenomen communicatie of gegevens over te schrijven of weer te geven. Het verzoek dat gericht is tot de onderzoeksrechter, wordt behandeld overeenkomstig artikel 61*quinquies*.

De rechter kan het verzoek afwijzen indien hij de raadpleging of de overschrijving of weergave van bijkomende delen niet noodzakelijk acht om de waarheid aan de dag te brengen, indien hij dit op dat ogenblik nadelig acht voor het onderzoek, of om redenen die verband houden met de bescherming van andere rechten of belangen van personen. Hij kan de raadpleging of de overschrijving of weergave van bijkomende delen ook beperken tot een door hem nader omschreven selectie van bestanden of stukken.".

L'inculpé, le prévenu, la partie civile ou leurs conseils peuvent demander au juge d'instruction de consulter au greffe les autres fichiers ou pièces déposés conformément au § 4 au greffe ou à la police fédérale, ainsi que de transcrire ou reproduire des parties supplémentaires des communications ou données enregistrées. La demande, adressée au juge d'instruction, est traitée conformément à l'article 61*quinquies*.

Le juge d'instruction peut en outre reje*ter* cette demande s'il estime que la consultation, la transcription ou la reproduction des parties supplémentaires n'est pas nécessaire à la manifestation de la vérité, s'il le juge à ce moment préjudiciable à l'enquête ou pour des raisons liées à la protection d'autres droits ou intérêts de personnes. Il peut également limiter la consultation ou la transcription ou reproduction de parties supplémentaires à une sélection de fichiers ou pièces qu'il détermine.".

Artikel 22

Artikel 90*octies* van hetzelfde Wetboek, ingevoegd bij de wet van 30 juni 1994, wordt vervangen als volgt:

"Art. 90*octies*. § 1. De maatregel kan alleen betrekking hebben op de lokalen aangewend voor beroepsdoeleinden, de woonplaats, de communicatiemiddelen of de informaticasystemen van een advocaat of een arts, indien deze er zelf van verdacht worden een van de strafbare feiten bedoeld in artikel 90*ter* te hebben gepleegd of eraan deelgenomen te hebben, of, indien precieze feiten doen vermoeden dat derden die ervan verdacht worden een van de strafbare feiten bedoeld in artikel 90*ter* te hebben gepleegd, gebruik maken van diens lokalen, woonplaats, communicatiemiddelen of informaticasystemen.

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

Deze personen zijn tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

§ 3. De onderzoeksrechter beoordeelt, na overleg met de stafhouder of de vertegenwoordiger van de provinciale orde van geneesheren, welke gedeelten van de in artikel 90*sexies*, § 3, bedoelde niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem, die hij van belang acht voor het onderzoek, onder het beroepsgeheim vallen en welke niet.

Enkel de gedeelten van de communicatie of gegevens bedoeld in het vorige lid die worden geacht niet onder het beroepsgeheim te vallen, worden overgeschreven of weergegeven en worden desgevallend vertaald. De onderzoeksrechter laat hiervan proces-verbaal opmaken. De bestanden bevattende deze communicatie of gegevens worden onder verzegelde omslag neergelegd ter griffie.

Article 22

L'article 90*octies* du même Code, inséré par la loi du 30 juin 1994, est remplacé par ce qui suit:

"Art. 90*octies*. § 1er. La mesure ne pourra por*ter* sur les locaux utilisés à des fins professionnelles, la résidence, les moyens de communication ou les systèmes informatiques d'un avocat ou d'un médecin que si celui-ci est lui-même soupçonné d'avoir commis une des infractions visées à l'article 90*ter* ou d'y avoir participé, ou si des faits précis laissent présumer que des tiers soupçonnés d'avoir commis une des infractions visées à l'article 90*ter*, utilisent ses locaux, sa résidence, ses moyens de communication ou ses systèmes informatiques.

§ 2. 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 personnes sont tenues au secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

§ 3. Le juge d'instruction évalue, après concertation avec le bâtonnier ou le représentant de l'ordre provincial des médecins, quelles parties des communications non accessibles au public ou données d'un système informatique visées à l'article 90*sexies*, § 3, qu'il estime pertinentes pour l'instruction, relèvent du secret professionnel et quelles sont celles qui n'en relèvent pas.

Seules les parties des communications ou données visées à l'alinéa précédent qui sont estimées ne pas relever du secret professionnel sont transcrites ou reproduites et, le cas échéant, traduites. Le juge d'instruction en fait dresser procès-verbal. Les fichiers contenant ces communications ou données sont déposés au greffe sous pli scellé.

Alle overige communicatie of gegevens worden in een ander bestand onder afzonderlijke verzegelde omslag neergelegd ter griffie.".

Artikel 23

Artikel 90*novies* van hetzelfde Wetboek, ingevoegd bij de wet van 30 juni 1994 en gewijzigd bij de wet van 19 december 2002, wordt aangevuld met de woorden ", tenzij diens identiteit of woonplaats redelijkerwijze niet achterhaald kan worden.".

Artikel 24

In 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, 6 januari 2003 en … (dataretentiewet), wordt het derde lid vervangen als volgt:

"Hij brengt tegelijkertijd verslag uit over de toepassing van de artikelen 40*bis*, 46*ter*, 46*quater*, 46*quinquies*, 47*ter* tot 47*decies*, 56*bis*, 86*bis*, 86*ter*, 88*sexies*, en 89*ter*.".

Artikel 25

In artikel 235*ter* van hetzelfde Wetboek, ingevoegd bij de wet van 27 december 2005 en gewijzigd bij de wetten van 16 januari 2009, 29 januari 2016 en 5 februari 2016, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1 wordt het eerste lid aangevuld met de woorden ", en over de toepassing van de maatregel bedoeld in artikel 46*sexies* indien daarbij een vertrouwelijk dossier werd aangelegd.";

2° in paragraaf 1, tweede lid, worden de woorden "en van de maatregel bedoeld in artikel 46*sexies*" ingevoegd tussen de woorden "observatie en infiltratie" en de woorden "bij het afsluiten van het opsporingsonderzoek";

3° in paragraaf 1, derde lid, worden de woorden "en van de maatregel bedoeld in artikel 46*sexies*" ingevoegd tussen de woorden "observatie en infiltratie" en de woorden "die werden toegepast";

4° in paragraaf 2 worden het vierde en het vijfde lid vervangen als volgt:

"Zij kan, met betrekking tot de toegepaste bijzondere opsporingsmethoden observatie en infiltratie en de maatregel bedoeld in artikel 46*sexies*, de onderzoeksrechter, de in de artikelen 47*sexies*, § 3, 6° en 47*octies*, § 3, 6° bedoelde officier van gerechtelijke politie, en de officier van gerechtelijke politie belast met de leiding over de uitvoering van de maatregel bedoeld in artikel 46*sexies*, afzonderlijk en buiten de aanwezigheid van de partijen horen.

De kamer van inbeschuldigingstelling kan de onderzoeksrechter gelasten de politieambtenaren die belast zijn met de

Toutes les autres communications ou données sont déposées au greffe dans un autre fichier sous pli scellé séparé.".

Article 23

L'article 90*novies* du même Code, inséré par la loi du 30 juin 1994 et modifié par la loi du 19 décembre 2002, est complété par les mots ", sauf si son identité ou son adresse ne peut être raisonnablement retrouvée.".

Article 24

A 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, 6 janvier 2003 et … (loi data retention), l'alinéa 3 est remplacé par ce qui suit:

"Il fait en même temps rapport sur l'application des articles 40*bis*, 46*ter*, 46*quater*, 46*quinquies*, 47*ter* à 47*decies*, 56*bis*, 86*bis*, 86*ter*, 88*sexies* et 89*ter*.".

Article 25

A l'article 235*ter* du même Code, inséré par la loi du 27 décembre 2005 et modifié par les lois du 16 janvier 2009, 29 janvier 2016 et 5 février 2016, les modifications suivantes sont apportées:

1° dans le paragraphe 1er, l'alinéa 1 est complété par les mots "et l'application de la mesure visée à l'article 46*septies* si un dossier confidentiel a été ouvert dans ce cadre.";

2° dans le paragraphe 1, l'alinéa 2 est complété par les mots "et de la mesure visée à l'article 46*sexies*.";

3° dans le paragraphe 1, l'alinéa 3, les mots "et de la mesure visée à l'article 46*sexies*" sont insérés entre les mots "d'observation et d'infiltration" et les mots "qui ont été appliquées";

4° dans le paragraphe 2, les alinéas 4 et 5 sont remplacés par ce qui suit:

"Pour les méthodes particulières de recherche d'observation et d'infiltration et la mesure visée à l'article 46*sexies*, elle peut entendre, séparément et en l'absence des parties, le juge d'instruction et l'officier de police judiciaire visé aux articles 47*sexies*, § 3, 6°, et 47*octies*, § 3, 6°, et l'officier de police judiciaire chargé de diriger la mise en œuvre de la mesure visée à l'article 46*sexies*.

La chambre des mises en accusation peut charger le juge d'instruction d'entendre les fonctionnaires de police chargés

uitvoering van de observatie en infiltratie, en de in artikel 47*octies*, § 1, tweede lid, bedoelde burger, de politieambtenaren belast met de uitvoering van de maatregel bedoeld in artikel 46*sexies*, en de in artikel 46*sexies*, § 1, tweede lid bedoelde burger te horen met toepassing van de artikelen 86*bis* en 86*ter*. Zij kan beslissen bij het verhoor door de onderzoeksrechter aanwezig te zijn of één van haar leden daartoe af te vaardigen.";

5° in paragraaf 3, eerste lid, worden de woorden "de artikelen 47*septies*, § 1, tweede lid, of 47*novies*, § 1, tweede lid," vervangen door de woorden "de artikelen 46*sexies*, § 3, zevende lid, 47*septies*, § 1, tweede lid, of 47*novies*, § 1, tweede lid,";

6° in paragraaf 4 worden de woorden "de observatie of infiltratie en de in artikel 47*octies*, § 1, tweede lid, bedoelde burger" vervangen door de woorden "de observatie, de infiltratie of de maatregel bedoeld in artikel 46*sexies*, en de in de artikelen 47*octies*, § 1, tweede lid en 46*sexies*, § 1, tweede lid bedoelde burger".

Artikel 26

In artikel 235*quater* van hetzelfde Wetboek, ingevoerd bij de wet van 27 december 2005, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1, eerste lid, worden de woorden "en van de maatregel bedoeld in artikel 46*sexies* indien daarbij een vertrouwelijk dossier werd aangelegd," ingevoegd tussen de woorden "observatie en infiltratie" en de woorden "die werden toegepast";

2° in paragraaf 1, tweede lid, worden de woorden "over de dossiers waarvoor tot observaties en infiltraties werd beslist door het openbaar ministerie of door de onderzoeksrechter" vervangen door de woorden "over de dossiers waarvoor door het openbaar ministerie of door de onderzoeksrechter werd beslist tot observaties en infiltraties en tot de maatregel bedoeld in artikel 46*sexies* indien daarbij een vertrouwelijk dossier werd aangelegd";

3° paragraaf 2, tweede lid, wordt vervangen als volgt:

"Zij kan, met betrekking tot de toegepaste bijzondere opsporingsmethoden observatie of infiltratie en de maatregel bedoeld in artikel 46*sexies*, de onderzoeksrechter, de in de artikelen 47*sexies*, § 3, 6°, en 47*octies*, § 3, 6°, bedoelde officier van gerechtelijke politie en de officier van gerechtelijke politie belast met de leiding over de uitvoering van de maatregel bedoeld in artikel 46*sexies* afzonderlijk en buiten de aanwezigheid van de partijen horen.";

4° in paragraaf 3, eerste lid, worden de woorden "de artikelen 47*septies*, § 1, tweede lid, of 47*novies*, § 1, tweede lid" vervangen door de woorden "de artikelen 47*septies*, § 1, tweede lid, 47*novies*, § 1, tweede lid of 46*sexies*, § 3, zevende lid";

5° in paragraaf 4 worden de woorden "de observatie of infiltratie en de in artikel 47*octies*, § 1, tweede lid, bedoelde

d'exécuter l'observation et l'infiltration, le civil visé à l'article 47*octies*, § 1er, alinéa 2, en application des articles 86*bis* et 86*ter*, les fonctionnaires de police chargés de la mise en œuvre de la mesure visée à l'article 46*sexies* et le civil visé à l'article 46*sexies*, § 1er, alinéa 2. Elle peut décider d'être présente à l'audition menée par le juge d'instruction ou de déléguer un de ses membres à cet effet.";

5° dans le paragraphe 3, l'alinéa 1er les mots "aux articles 47*septies*, § 1er, alinéa 2, ou 47*novies*, § 1er, alinéa 2," sont remplacés par les mots "aux articles 46*sexies*, § 3, alinéa 7, 47*septies*, § 1er, alinéa 2, ou 47*novies*, § 1er, alinéa 2,";

6° dans le paragraphe 4 les mots "de l'observation ou de l'infiltration et du civil visé à l'article 47*octies*, § 1er, alinéa 2" sont remplacés par les mots "de l'observation, de l'infiltration ou de la mesure visée à l'article 46*sexies*, et du civil visé aux articles 47*octies*, § 1er, alinéa 2, et 46*sexies*, § 1er, alinéa 2".

Article 26

A l'article 235*quater* du même Code, inséré par la loi du 27 décembre 2005, les modifications suivantes sont apportées:

1° dans le paragraphe 1er, l'alinéa 1er, les mots "et de la mesure visée à l'article 46*sexies* si un dossier confidentiel a été ouvert dans ce cadre," sont insérés entre les mots "d'observation et d'infiltration" et les mots "qui ont été appliquées";

2° dans le paragraphe 1, l'alinéa 2, les mots "pour lesquels des observations et des infiltrations ont été décidées par le ministère public ou par le juge d'instruction" sont remplacés par les mots "pour lesquels des observations et des infiltrations et la mesure visée à l'article 46*sexies*, si un dossier confidentiel a été ouvert dans ce cadre, ont été décidées par le ministère public ou par le juge d'instruction";

3° paragraphe 2, l'alinéa 2, est remplacé par ce qui suit:

"Pour les méthodes particulières de recherche d'observation ou d'infiltration et la mesure visée à l'article 46*sexies*, elle peut entendre, séparément et en l'absence des parties, le juge d'instruction et l'officier de police judiciaire visé aux articles 47*sexies*, § 3, 6°, et 47*octies*, § 3, 6°, et l'officier de police judiciaire chargé de diriger la mise en œuvre de la mesure visée à l'article 46*sexies*.";

4° dans le paragraphe 3, alinéa 1er, les mots "aux articles 47*septies*, § 1er, alinéa 2, ou 47*novies*, § 1er, alinéa 2" sont remplacés par les mots "aux articles 47*septies*, § 1er, alinéa 2, 47*novies*, § 1er, alinéa 2, ou 46*sexies*, § 3, alinéa 7";

5° dans le paragraphe 4 les mots "de l'observation ou de l'infiltration et du civil visé à l'article 47*octies*, § 1er, alinéa 2"

burger" vervangen door de woorden "de observatie, de infiltratie of de maatregel bedoeld in artikel 46*sexies*, en de in de artikelen 47*octies*, § 1, tweede lid en 46*sexies*, § 1, tweede lid bedoelde burger".

Artikel 27

In artikel 464/13 van hetzelfde Wetboek, ingevoegd bij de wet van 11 februari 2014 worden de volgende wijzigingen aangebracht:

1° paragraaf 1 wordt vervangen als volgt:

"§ 1. De SUO-magistraat of de gevorderde politiedienst kan bij een schriftelijke en met redenen omklede beslissing, van de actoren bedoeld in het tweede lid de mededeling van de volgende inlichtingen vorderen:

1° de identificatie van een abonnee of een gewoonlijke gebruiker van een dienst zoals bedoeld in het tweede lid, tweede streepje, of van het gebruikte elektronische communicatiemiddel;

2° de identificatie van de diensten zoals bedoeld in het tweede lid, tweede streepje, waarop een bepaalde persoon geabonneerd is of die door een bepaalde persoon gewoonlijk worden gebruikt.

De volgende actoren zijn gehouden tot medewerking overeenkomstig het vorige lid:

— de operator van een elektronisch communicatienetwerk; en

— iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.";

2° paragraaf 2 wordt vervangen als volgt:

"§ 2. De actoren bedoeld in § 1, tweede lid, verstrekken alle beschikbare inlichtingen in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de beslissing, volgens de modaliteiten die bepaald worden bij het ter uitvoering van artikel 46*bis*, § 2, eerste en tweede lid, genomen koninklijk besluit.

Iedere persoon die de gegevens weigert mee te delen of deze niet meedeelt in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de beslissing, wordt gestraft met geldboete van zesentwintig euro tot tienduizend euro."

sont remplacés par les mots "de l'observation, de l'infiltration ou de la mesure visée à l'article 46*sexies*, et du civil visé aux articles 47*octies*, § 1er, alinéa 2, et 46*sexies*, § 1er, alinéa 2".

Article 27

A l'article 464/13 du même Code, inséré par la loi de 11 février 2014, les modifications suivantes sont apportées:

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

"§ 1er. Le magistrat EPE ou le service de police requis peut, par décision écrite et motivée, requérir les acteurs visés à l'alinéa 2 de lui communiquer les renseignements suivants:

1° l'identification d'un abonné ou d'un utilisateur habituel d'un service visé à l'alinéa 2, deuxième tiret, ou bien du moyen de communication électronique utilisé;

2° l'identification des services visés à l'alinéa 2, deuxième tiret, auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée.

Les acteurs suivants sont tenus de collaborer conformément à l'alinéa précédent:

— l'opérateur d'un réseau de communications électroniques; et

— toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.";

2° le paragraphe 2 est remplacé par ce qui suit:

"§ 2. Les acteurs visés au § 1er, alinéa 2, fournissent tous les renseignements disponibles en temps réel ou, le cas échéant, au moment précisé dans la décision, selon les modalités fixées par l'arrêté royal pris en exécution de l'article 46*bis*, § 2, alinéas 1er et 2.

Toute personne qui refuse de communiquer les données ou qui ne les communique pas en temps réel ou, le cas échéant, au moment précisé dans la réquisition est punie d'une amende de vingt-six euros à dix mille euros.".

Artikel 28

In artikel 464/25 van hetzelfde Wetboek, ingevoegd bij de wet van 11 februari 2014 worden de volgende wijzigingen aangebracht:

1° in paragraaf 1, eerste lid, worden de woorden “de actoren bedoeld in het tweede lid” ingevoegd tussen de woorden “de gevorderde politiedienst kan” en “vorderen om”;

2° in paragraaf 1 wordt tussen het eerste en het tweede lid een lid ingevoegd, luidende:

“De volgende actoren zijn gehouden tot medewerking overeenkomstig het vorige lid:

— de operator van een elektronisch communicatienetwerk; en

— iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.”;

3° paragraaf 2 wordt vervangen als volgt:

“§ 2. De actoren bedoeld in § 1, tweede lid delen de gevorderde inlichtingen mee in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de beslissing, volgens de modaliteiten die bepaald worden bij het ter uitvoering van artikel 88*bis*, § 2, eerste en derde lid, genomen koninklijk besluit.

Iedere persoon die zijn technische medewerking aan de in dit artikel bedoelde vorderingen weigert of niet verleent in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de beslissing, wordt gestraft met een geldboete van zesentwintig euro tot tienduizend euro.”.

TITEL 3

Bepalingen tot wijziging van het Strafwetboek

Artikel 29

In het Strafwetboek wordt het opschrift van Boek 2, Titel IV, Hoofdstuk V*bis* vervangen als volgt:

“Boek 2, Titel IV, Hoofdstuk V*bis.* Onderscheppen, kennisnemen en opnemen van niet voor het publiek toegankelijke communicatie en gegevens van een informaticasysteem”.

Article 28

A l’article 464/25 du même Code, inséré par la loi de 11 février 2014 les modifications suivantes sont apportées:

1° dans le paragraphe 1, alinéa 1, les mots “les acteurs visés à l’alinéa 2” sont insérés entre les mots “le service de police requis peut requérir” et les mots “de faire procéder”;

2° dans le paragraphe 1, un alinéa rédigé comme suit est inséré entre les alinéas 1 et 2:

“Les acteurs suivants sont tenus de collaborer conformément à l’alinéa précédent:

— l’opérateur d’un réseau de communications électroniques; et

— toute personne qui met à disposition ou offre, sur le territoire belge, d’une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d’un service de communications électroniques.”;

3° le paragraphe 2 est remplacé par ce qui suit:

“§ 2. Les acteurs visés au § 1er, alinéa 2, communiquent les renseignements requis en temps réel ou, le cas échéant, au moment précisé dans la décision, selon les modalités fixées par l’arrêté royal pris en exécution de l’article 88*bis*, § 2, alinéas 1er et 3.

Toute personne qui refuse de prêter son concours technique aux réquisitions visées dans le présent article ou ne le prête pas en temps réel ou, le cas échéant, au moment précisé dans la décision est punie d’une amende de vingt-six euros à dix mille euros.”.

TITRE 3

Dispositions modifiant le Code pénal

Article 29

Dans le Code pénal, l’intitulé du Livre 2, Titre IV, Chapitre V*bis* est remplacé par ce qui suit:

“Interception, prise de connaissance et enregistrement de communications non accessibles au public et de données d’un système informatique”.

Artikel 30

In artikel 259*bis* van hetzelfde wetboek, ingevoegd bij de wet van 30 juni 2004, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1 wordt de bepaling onder 1° vervangen als volgt:

"1° ofwel, opzettelijk, met behulp van enig toestel niet voor publiek toegankelijke communicatie, waaraan hij niet deelneemt, onderschept of doet onderscheppen, er kennis van neemt of doet van nemen, opneemt of doet opnemen, zonder de toestemming van alle deelnemers aan die communicatie";

2° in paragraaf 1 wordt de bepaling onder 3° vervangen als volgt:

"3° ofwel, wetens, de inhoud van niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem die onwettig onderschept of opgenomen zijn of waarvan onwettig kennis genomen is, onder zich houdt, aan een andere persoon onthult of verspreidt, of wetens enig gebruik maakt van een op die manier verkregen inlichting.";

3° in paragraaf 2 worden de woorden "een wettig gemaakte opname van privécommunicatie of –telecommunicatie" vervangen door de woorden "een wettig gemaakte opname van niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem.".

Artikel 31

In hetzelfde wetboek wordt het opschrift van Boek 2, Titel V, Hoofdstuk VIII*bis* vervangen als volgt:

"Boek 2, Titel V, Hoofdstuk VIII*bis*. Misdrijven betreffende het geheim van niet voor het publiek toegankelijke communicatie en gegevens van een informaticasysteem".

Artikel 32

In artikel 314*bis* van hetzelfde wetboek worden de volgende wijzigingen aangebracht:

1° in paragraaf 1 wordt de bepaling onder 1° vervangen als volgt:

"1° ofwel, opzettelijk, met behulp van enig toestel niet voor publiek toegankelijke communicatie, waaraan hij niet deelneemt, onderschept of doet onderscheppen, er kennis van neemt of doet van nemen, opneemt of doet opnemen, zonder de toestemming van alle deelnemers aan die communicatie;";

2° paragraaf 2 wordt vervangen als volgt:

"§ 2. Met gevangenisstraf van zes maanden tot twee jaar en met geldboete van vijfhonderd [euro] tot twintigduizend [euro] of met een van die straffen alleen wordt gestraft hij,

Article 30

A l'article 259*bis* du même Code, inséré par la loi de 30 juin 2004, les modifications suivantes sont apportées:

1°dans le paragraphe 1, le 1° est remplacé par ce qui suit:

"1° soit, intentionnellement, à l'aide d'un appareil quelconque, intercepte ou fait intercepter, prend connaissance ou fait prendre connaissance, enregistre ou fait enregistrer des communications non accessibles au public, auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications";

2° dans le paragraphe 1, le 3° est remplacé par ce qui suit:

"3° soit, sciemment, détient, révèle ou divulgue à une autre personne le contenu de communications non accessibles au public ou de données d'un système informatique illégalement interceptées ou enregistrées, ou dont il a pris connaissance illégalement, ou utilise sciemment d'une manière quelconque une information obtenue de cette façon.";

3° dans le paragraphe 2 les mots "de communications ou de télécommunications privées" sont remplacés par les mots "de communications non accessibles au public ou de données d'un système informatique.".

Article 31

Dans le même code, l'intitulé du Livre 2, Titre V, Chapitre VII*bis* est remplacé par ce qui suit:

"Livre 2, Titre V, Chapitre VIII*bis*.another Infractions relatives au secret des communications non accessibles au public et des données d'un système informatique".

Article 32

A l'article 314*bis* du même Code, les modifications suivantes sont apportées:

1°dans le paragraphe 1, le 1° est remplacé par ce qui suit:

"1° soit, intentionnellement, à l'aide d'un appareil quelconque, intercepte ou fait intercepter, prend connaissance ou fait prendre connaissance, enregistre ou fait enregistrer des communications non accessibles au public, auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications;";

2° le paragraphe 2 est remplacé par ce qui suit:

"§ 2. Sera puni d'un emprisonnement de six mois à deux ans et d'une amende de cinq cents [euros] à vingt mille [euros] ou d'une de ces peines seulement, quiconque détient, révèle

die wetens, de inhoud van niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem die onwettig onderschept of opgenomen zijn of waarvan onwettig kennis genomen is, onder zich houdt, aan een andere persoon onthult of verspreidt, of wetens enig gebruik maakt van een op die manier verkregen inlichting.

Met dezelfde straffen wordt gestraft hij die, met bedrieglijk opzet of met het oogmerk te schaden, gebruik maakt van een wettig gemaakte opname van niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem.".

ou divulgue sciemment à une autre personne le contenu de communications non accessibles au public et de données d'un système informatique illégalement interceptées ou enregistrées, ou dont il a pris connaissance illégalement, ou utilise sciemment d'une manière quelconque une information obtenue de cette façon.

Sera puni des mêmes peines quiconque, avec une intention frauduleuse ou à dessein de nuire, utilise un enregistrement, légalement effectué, de communications non accessibles au public ou de données d'un système informatique.".

TITEL 4

Bepaling tot de oprichting van een gegevensbank stemafdrukken

TITRE 4

Disposition pour la création d'une banque de données des empreintes vocales

Artikel 33

De technische gegevens die het mogelijk maken de stem te herkennen van de personen, die het voorwerp uitmaken of hebben uitgemaakt van een maatregel tot interceptie bedoeld in artikel 90*ter*, § 1, van het Wetboek van Strafvordering en die bedoeld worden in artikel 44/5, § 3, 1° van de wet van 5 augustus 1992 op het politieambt, worden gedurende ten hoogste 10 jaar bewaard in de Algemene Nationale Gegevensbank bedoeld in dezelfde wet, met het oog op de identificatie van die personen in het kader van afluisterdossiers uitgevoerd op verzoek van de gerechtelijke overheden.

Behalve die technische gegevens bevat deze gegevensbank ook de gegevens over het dossiernummer, de bevoegde magistraat en het bedoelde gerechtelijke arrondissement.

De in het eerste lid bedoelde technische gegevens verschillen van de opnames die worden gemaakt in het kader van de tenuitvoerlegging van de maatregel bedoeld in artikel 90*ter* van het Wetboek van Strafvordering. Die opnames worden niet beoogd door dit artikel.

De doeleinden en nadere regels voor de verwerking van die gegevens worden bepaald in de artikelen 44/7 tot 44/11/1 van de wet van 5 augustus 1992 op het politieambt.

Article 33

Les données techniques permettant la reconnaissance vocale des personnes, faisant ou ayant fait l'objet d'une mesure d'interception des télécommunications visée à l'article 90*ter*, § 1 du Code d'instruction criminelle et qui sont visées à l'article 44/5, § 3, 1° de la loi de 5 août 1992 sur la fonction de police, sont conservées pendant 10 ans au maximum dans la Banque de données Nationale Générale visée dans la même loi, en vue d'aider à identifier ces personnes dans le cadre de dossiers d'écoute réalisés à la demande des autorités judiciaires.

Outre ces données techniques, cette banque de données contient également les données relatives au numéro de dossier, au magistrat compétent et à l'arrondissement judiciaire visé.

Les données techniques visées au premier alinéa sont distinctes des enregistrements réalisés dans le cadre de la mise en œuvre de la mesure visée à l'article 90*ter*, § 1 du Code d'instruction criminelle. Ces enregistrements ne sont pas concernés par le présent article.

Les finalités et les modalités de traitement de ces données sont celles prévues aux articles 44/7 à 44/11/1 de la loi de 5 août 1992 sur la fonction de police.

Geïntegreerde impactanalyse

Beschrijvende fiche

A. Auteur

Bevoegd regeringslid

Koen Geens, Jan Jambon

Contactpersoon beleidscel

Overheidsdienst

FOD Justitie

Contactpersoon overheidsdienst

B. Ontwerp

Titel van de regelgeving

Voorontwerp van wet betreffende de verbetering van de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden

Korte beschrijving van het ontwerp van regelgeving met vermelding van de oorsprong (verdrag, richtlijn, samenwerkingsakkoord, actualiteit, …), de beoogde doelen van uitvoering.

Het voorontwerp van wet bevat een aantal wijzigingen in het Wetboek van Strafvordering en beoogt een aantal verbeteringen aan te brengen in het opsporingsonderzoek en het gerechtelijk onderzoek. Dit is nodig gezien de recente actualiteit.

Impactanalyses reeds uitgevoerd:

☐ Ja ■ Nee

C. Raadpleging over het ontwerp van regelgeving

Verplichte, facultatieve of informele raadplegingen

Het voorontwerp werd uitgewerkt in samenwerking met gespecialiseerde magistraten en afgevaardigden van de Federale Politie, het SAT, de douane, een lid van de beleidscel van de Minister van Justitie en één van Binnenlandse zaken, juristen en criminologen van de FOD Justitie.
Privacycommissie, IF, Raad van State.

D. Bronnen gebruikt om de impactanalyse uit te voeren

Statistieken, referentiedocumenten, organisaties en referentiepersonen

/

Welke impact heeft het ontwerp van regelgeving op deze 21 thema's?

1. Kansarmoedebestrijding

☐ Positieve impact ☐ Negatieve impact | ■ Geen impact

2. Gelijke kansen en sociale cohesie

☐ Positieve impact ☐ Negatieve impact | ■ Geen impact

3. Gelijkheid van vrouwen en mannen

1. Op welke personen heeft het ontwerp (rechtstreeks of onrechtstreeks) een impact en wat is de naar geslacht uitgesplitste samenstelling van deze groep(en) van personen?

■ Er zijn personen betrokken. | ☐ Personen zijn niet betrokken.

Beschrijf en meld de % vrouwen-mannen aan:

Het wetsontwerp van wet is van toepassing op alle natuurlijke personen en rechtspersonen. Een uitsplitsing naar geslacht is niet mogelijk.

2. Identificeer de eventuele verschillen in de respectieve situatie van vrouwen en mannen binnen de materie waarop het ontwerp van regelgeving betrekking heeft.

Niet van toepassing

☐ Vink dit aan indien er verschillen zijn.

4. Gezondheid

☐ Positieve impact ☐ Negatieve impact | ■ Geen impact

5. Werkgelegenheid

☐ Positieve impact ☐ Negatieve impact | ■ Geen impact

6. Consumptie- en productiepatronen

☐ Positieve impact ☐ Negatieve impact | ■ Geen impact

7. Economische ontwikkeling

☐ Positieve impact ☐ Negatieve impact | ■ Geen impact

8. Investeringen

☐ Positieve impact ☐ Negatieve impact | ■ Geen impact

9. Onderzoek en ontwikkeling

☐ Positieve impact ☐ Negatieve impact | ■ Geen impact

10. Kmo's

1. Welke ondernemingen zijn rechtstreeks of onrechtstreeks betrokken?

☐ Er zijn ondernemingen (inclusief kmo's) betrokken. | ■ Ondernemingen zijn niet betrokken.

Leg uit waarom:

Het voorontwerp van wet heeft betrekking op de strafrechtelijke aansprakelijkheid van natuurlijke personen en rechtspersonen; geen impact op de ontwikkeling van de rechtspersonen.

11. Administratieve lasten

☐ Ondernemingen of burgers zijn betrokken. ☒ Ondernemingen of burgers zijn niet betrokken.

12. Energie

☐ Positieve impact ☐ Negatieve impact ☒ Geen impact

13. Mobiliteit

☐ Positieve impact ☐ Negatieve impact ☒ Geen impact

14. Voeding

☐ Positieve impact ☐ Negatieve impact ☒ Geen impact

15. Klimaatverandering

☐ Positieve impact ☐ Negatieve impact ☒ Geen impact

16. Natuurlijke hulpbronnen

☐ Positieve impact ☐ Negatieve impact ☒ Geen impact

17. Buiten- en binnenlucht

☐ Positieve impact ☐ Negatieve impact ☒ Geen impact

18. Biodiversiteit

☐ Positieve impact ☐ Negatieve impact ☒ Geen impact

19. Hinder

☐ Positieve impact ☐ Negatieve impact ☒ Geen impact

20. Overheid

☐ Positieve impact ☐ Negatieve impact ☒ Geen impact

21. Beleidscoherentie ten gunste van ontwikkeling

1. Identificeer de eventuele rechtstreekse of onrechtstreekse impact van het ontwerp op de ontwikkelingslanden op het vlak van: voedselveiligheid, gezondheid en toegang tot geneesmiddelen, waardig werk, lokale en internationale handel, inkomens en mobilisering van lokale middelen (taxatie), mobiliteit van personen, leefmilieu en klimaatverandering (mechanismen voor schone ontwikkeling), vrede en veiligheid.

☐ Impact op ontwikkelingslanden. ☒ Geen impact op ontwikkelingslanden.

Leg uit waarom:

/

Analyse d'impact intégrée

Fiche signalétique

A. Auteur

Membre du Gouvernement compétent

Koen Geens, Jan Jambon

Contact cellule stratégique

Administration

SPF Justice

Contact administration

B. Projet

Titre de la règlementation

Avant-projet de loi relative à l'amélioration des méthodes particulières de recherche et de quelques autres méthodes d'enquête

Description succincte du projet de réglementation en mentionnant l'origine réglementaire (traités, directive, accord de coopération, actualité, …), les objectifs poursuivis et la mise en œuvre.

L'avant-projet de loi contient un certain nombre de modifications apportées au Code d'Instruction criminelle et vise à apporter un certain nombre d'améliorations dans le cadre de l'information et de l'instruction. Vu l'actualité récent, ces changements sont nécessaires.

Analyses d'impact déjà réalisées :

☐ Oui ■ Non

C. Consultations sur le projet de réglementation

Consultation obligatoire, facultative ou informelle

L'avant-projet a été élaboré en collaboration avec des magistrats spécialisés et des réprésentants de la Police Fédéral, le SAT, la douane, un membre de la Cellule stratégique du Ministre de la Justice et un de l'Intérieur, de juristes et de criminologues du SPF Justice.
Commission vie privé, IF, Conseil d'Etat.

D. Sources utilisées pour effectuer l'analyse d'impact

Statistiques, documents, institutions et personnes de référence

/

Avant-projet de loi relative à l'amélioration des méthodes particulières de recherche et de quelques autres méthodes d'enquête - (v1) - 01/12/2015 10:34

Quel est l'impact du projet de réglementation sur ces 21 thèmes ?

1. Lutte contre la pauvreté

☐ Impact positif ☐ Impact négatif | ☒ Pas d'impact

2. Égalité des chances et cohésion sociale

☐ Impact positif ☐ Impact négatif | ☒ Pas d'impact

3. Égalité des femmes et des hommes

1. Quelles personnes sont (directement et indirectement) concernées par le projet et quelle est la composition sexuée de ce(s) groupe(s) de personnes ?

☒ Des personnes sont concernées. | ☐ Aucune personne n'est concernée.

Décrivez et indiquez le % femmes-hommes :

L'avant-projet de loi est applicable à toute personne physique et morale. Une répartition par sexe n'est pas possible.

2. Identifiez les éventuelles différences entre la situation respective des femmes et des hommes dans la matière relative au projet de réglementation.

N/a

☐ S'il existe des différences, cochez cette case.

4. Santé

☐ Impact positif ☐ Impact négatif | ☒ Pas d'impact

5. Emploi

☐ Impact positif ☐ Impact négatif | ☒ Pas d'impact

6. Modes de consommation et production

☐ Impact positif ☐ Impact négatif | ☒ Pas d'impact

7. Développement économique

☐ Impact positif ☐ Impact négatif | ☒ Pas d'impact

8. Investissements

☐ Impact positif ☐ Impact négatif | ☒ Pas d'impact

9. Recherche et développement

☐ Impact positif ☐ Impact négatif | ☒ Pas d'impact

10. PME

1. Quelles entreprises sont directement et indirectement concernées ?

☐ Des entreprises (dont des PME) sont concernées. | ☒ Aucune entreprise n'est concernée.

Expliquez pourquoi :

L'avant-projet de loi a trait à la responsabilité pénale des personnes physiques et morales; pas d'impact sur le développement de ces dernières.

11. Charges administratives

☐ Des entreprises/citoyens sont concernés. ☒ Les entreprises/citoyens ne sont pas concernés.

12. Énergie

☐ Impact positif ☐ Impact négatif | ☒ Pas d'impact

13. Mobilité

☐ Impact positif ☐ Impact négatif | ☒ Pas d'impact

14. Alimentation

☐ Impact positif ☐ Impact négatif | ☒ Pas d'impact

15. Changements climatiques

☐ Impact positif ☐ Impact négatif | ☒ Pas d'impact

16. Ressources naturelles

☐ Impact positif ☐ Impact négatif | ☒ Pas d'impact

17. Air intérieur et extérieur

☐ Impact positif ☐ Impact négatif | ☒ Pas d'impact

18. Biodiversité

☐ Impact positif ☐ Impact négatif | ☒ Pas d'impact

19. Nuisances

☐ Impact positif ☐ Impact négatif | ☒ Pas d'impact

20. Autorités publiques

☐ Impact positif ☐ Impact négatif | ☒ Pas d'impact

21. Cohérence des politiques en faveur du développement

1. Identifiez les éventuels impacts directs et indirects du projet sur les pays en développement dans les domaines suivants : sécurité alimentaire, santé et accès aux médicaments, travail décent, commerce local et international, revenus et mobilisations de ressources domestiques (taxation), mobilité des personnes, environnement et changements climatiques (mécanismes de développement propre), paix et sécurité.

☐ Impact sur les pays en développement. | ☒ Pas d'imapct sur les pays en développement.

Expliquez pourquoi :

/

ADVIES VAN DE RAAD VAN STATE NR. 59.199/3 VAN 9 MEI 2016

Op 29 maart 2016 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 verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecommunicaties".

Het voorontwerp is door de derde kamer onderzocht op 19 april 2016. De kamer was samengesteld uit Jo Baert, kamervoorzitter, Jan Smets en Koen Muylle, staatsraden, Jan Velaers en Bruno Peeters, assessoren, en Annemie Goossens, griffier.

Het verslag is uitgebracht door Frédéric Vanneste, auditeur.

De overeenstemming tussen de Franse en de Nederlandse tekst van het advies is nagezien onder toezicht van Jo Baert, kamervoorzitter, en Jan Smets, staatsraad.

Het advies, waarvan de tekst hierna volgt, is gegeven op 9 mei 2016.

*

1. Met toepassing van artikel 84, § 3, eerste lid, van de wetten op de Raad van State, gecoördineerd op 12 januari 1973, heeft de afdeling Wetgeving zich toegespitst op het onderzoek van de bevoegdheid van de steller van de handeling,[1] van de rechtsgrond, alsmede van de vraag of aan de te vervullen vormvereisten is voldaan.[2]

*

STREKKING VAN HET VOORONTWERP

2. Het om advies voorgelegde voorontwerp van wet strekt ertoe de wettelijke regeling inzake de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot het internet en de elektronische en telecommunicaties te verbeteren en te vervolledigen.

[1] Aangezien het om een voorontwerp van wet gaat, wordt onder "rechtsgrond" de overeenstemming met de hogere rechtsnormen verstaan.

[2] Gelet op de toegemeten termijn, de omvang en de complexiteit van het ontwerp, het grote aantal andere aan termijnen gebonden adviesaanvragen, in een aanzienlijk aantal gevallen eveneens over complexe en omvangrijke ontwerpen, en het geringe aantal magistraten dat aan de afdeling Wetgeving is toegewezen, heeft de Raad van State niet op alle vlakken een diepgaand onderzoek van het ontwerp kunnen verrichten. Uit de vaststelling dat over een bepaling in dit advies niets wordt opgemerkt, mag niet zonder meer worden afgeleid dat er niets over kan worden opgemerkt en, indien er iets over wordt opgemerkt, dat er niets méér over op te merken valt. Het advies dient met dit voorbehoud te worden gelezen.

AVIS DU CONSEIL D'ÉTAT N° 59.199/3 DU 9 MAI 2016

Le 29 mars 2016 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 l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications

L'avant-projet a été examiné par la troisième chambre le 19 avril 2016. La chambre était composée de Jo Baert, président de chambre, Jan Smets et Koen Muylle, conseillers d'État, Jan Velaers et Bruno Peeters, assesseurs, et Annemie Goossens, greffier.

Le rapport a été présenté par Frédéric Vannesteauditeur

La concordance entre la version française et la version néerlandaise de l'avis a été vérifiée sous le contrôle de Jo Baert, président de chambre, et Jan Smetsconseiller d'État

L'avis, dont le texte suit, a été donné le 9 mai 2016.

*

1. En application de l'article 84, § 3, alinéa 1er, des lois sur le Conseil d'État, coordonnées le 12 janvier 1973, la section de législation a fait por*ter* son examen essentiellement sur la compétence de l'auteur de l'acte [1], le fondement juridique et l'accomplissement des formalités prescrites [2].

*

PORTÉE DE L'AVANT PROJET

2. L'avant-projet de loi soumis pour avis a pour objet d'améliorer et de compléter le dispositif législatif relatif aux méthodes particulières de recherche et à certaines mesures d'enquête concernant l'Internet, les communications électroniques et les télécommunications.

[1] S'agissant d'un avant-projet de loi, on entend par "fondement juridique" la conformité avec les normes supérieures.

[2] Eu égard au délai imparti, à l'ampleur et à la complexité du projet, au grand nombre d'autres demandes d'avis soumises à un délai, qui souvent portent également sur des projets complexes et volumineux, et au nombre restreint de magistrats affectés à la section de législation, le Conseil d'État n'a pas pu examiner tous les aspects du projet d'une manière approfondie. La circonstance qu'une disposition du projet ne fasse l'objet d'aucune observation dans le présent avis ne peut nullement signifier qu'il n'y a rien à observer à ce sujet, et si une observation est formulée, cela n'implique pas qu'elle est exhaustive. Il convient de lire l'avis sous cette réserve.

2.1. Artikel 39*bis* van het Wetboek van Strafvordering, dat grondig wordt herschreven, wordt voortaan het basisartikel op het vlak van de niet-heimelijke zoeking in informaticasystemen. Het wordt samengesmolten met artikel 88*ter* van dat wetboek, dat wordt opgeheven. In de memorie van toelichting wordt verduidelijkt dat erin het volgende wordt beoogd:

1° de zoeking waartoe een officier van gerechtelijke politie[3] kan beslissen, namelijk de zoeking in een informaticasysteem of in een deel ervan dat in beslag is genomen;

2° de door de procureur des Konings of de arbeidsauditeur[4] bevolen zoeking in een informaticasysteem dat niet in beslag is genomen, maar in beslag zou kunnen worden genomen;

3° de door de procureur des Konings of de arbeidsauditeur bevolen uitbreiding van een zoeking in een informaticasysteem dat op een andere plaats te lokaliseren is dan op de plaats waar de zoeking plaatsvindt. Die mogelijkheid, die thans nog in beginsel is voorbehouden aan de onderzoeksrechter, eventueel in het raam van het zogenaamde mini-onderzoek, wordt voortaan geregeld in artikel 39*bis*, § 4, van het Wetboek van Strafvordering. Tegelijk wordt de heimelijke zoeking in informaticasystemen ingevoerd, die is voorbehouden voor de onderzoeksrechter in het raam van het gerechtelijk onderzoek;

4° elke andere niet-heimelijke zoeking in een informaticasysteem. Dit soort zoeking kan enkel door een onderzoeksrechter worden bevolen.

Er wordt ook voorzien in begeleidende maatregelen om de in artikel 39*bis* van het Wetboek van Strafvordering bedoelde maatregelen mogelijk te maken.

2.2. In het Wetboek van Strafvordering worden, ter uitvoering van het Cybercrimeverdrag van de Raad van Europa van 23 november 2001 (hierna: het Cybercrimeverdrag),[5] nieuwe artikelen (39*ter* en 39*quater*) ingevoerd, die een procedure bevatten voor de bewaring van voor verlies of wijziging bijzonder kwetsbare gegevens, alsmede een regeling voor de bilaterale samenwerking tussen België en andere staten betreffende de snelle bewaring van gegevens.

2.3. De regeling met betrekking tot de identificatie van abonnees of gewoonlijke gebruikers van een elektronische communicatiedienst door de procureur des Konings of een officier van gerechtelijke politie wordt gewijzigd. Zo wordt het begrip "verstrekker van een elektronische communicatiedienst" nader bepaald en wordt voorzien in een aantal

[3] Met toepassing van artikel 56, § 1, derde lid, van het Wetboek van Strafvordering bezit ook de onderzoeksrechter de bevoegdheid om alle handelingen te verrichten die behoren tot de gerechtelijke politie of het opsporingsonderzoek. De procureur des Konings en de arbeidsauditeur zijn bovendien zelf officieren van gerechtelijke politie, die alle aan die officieren toegekende bevoegdheden ook zelf kunnen uitoefenen.

[4] Zie de vorige voetnoot.

[5] *Convention on Cybercrime*, gedaan te Boedapest op 23 november 2001, waarmee instemming is verleend bij de wet van 3 augustus 2012. Voor de Nederlandse vertaling, zie *BS* 21 november 2012, 69 093.

2.1. L'article 39*bis* du Code d'instruction criminelle, qui est fondamentalement remanié, devient désormais l'article de base pour ce qui regarde la recherche non secrète dans les systèmes informatiques. Il est fusionné avec l'article 88*ter* de ce code, qui est abrogé. L'exposé des motifs précise ce qui y est visé ainsi qu'il suit:

1° la recherche que peut ordonner un officier de police judiciaire [3], à savoir la recherche dans tout ou partie d'un système informatique saisi;

2° la recherche ordonnée par le procureur du Roi ou par l'auditeur du travail [4] dans un système informatique qui n'a pas été saisi, mais qui pourrait l'être;

3° l'extension, ordonnée par le procureur du Roi ou l'auditeur du travail, d'une recherche dans un système informatique qui se trouve à un autre endroit que celui où la recherche a lieu. Cette possibilité qui, actuellement, est encore en principe réservée au juge d'instruction, éventuellement dans le cadre de la "mini instruction", est désormais réglée à l'article 39*bis*, § 4, du Code d'instruction criminelle. Dans le même temps, la recherche en secret dans des systèmes informatiques, réservée au juge d'instruction dans le cadre de l'instruction, est introduite.

4° toute autre recherche non secrète dans un système informatique. Ce type de recherche ne peut être ordonné que par un juge d'instruction.

L'avant-projet prévoit également des mesures d'accompagnement en vue de permettre la mise en œuvre des mesures visées à l'article 39*bis* du Code d'instruction criminelle.

2.2. En exécution de la Convention du Conseil de l'Europe du 23 novembre 2001 sur la cybercriminalité (ci-après: la Convention cybercriminalité) [5] de nouveaux articles (39*ter* et 39*quater*) sont introduits dans le Code d'instruction criminelle, lesquels comportent une procédure visant à conserver des données particulièrement susceptibles de perte ou de modification, ainsi que des dispositions portant sur la collaboration bilatérale entre la Belgique et d'autres États en matière de conservation rapide de données.

2.3. La réglementation relative à l'identification des abonnés ou des utilisateurs habituels d'un service de communication électronique par le procureur du Roi ou un officier de police judiciaire est modifiée. C'est ainsi que la notion de "fournisseur d'un service de communications électroniques" est précisée et que le projet prévoit

[3] En application de l'article 56, § 1er, alinéa 3, du Code d'instruction criminelle, le juge d'instruction peut accomplir lui-même tous les actes qui relèvent de la police judiciaire ou de l'information. Le procureur du Roi et l'auditeur du travail sont en outre eux-mêmes des officiers de police judiciaire, qui peuvent également exercer eux-mêmes tous les pouvoirs qui sont attribués à ces officiers.

[4] Voir la note précédente.

[5] *Convention sur la cybercriminalité*, faite à Budapest le 23 novembre 2001, à laquelle la loi du 3 août 2012 a donné assentiment.

procedurele vereisten. Tevens wordt verduidelijkt dat de gevorderde medewerking “in werkelijke tijd [lees wellicht: onmiddellijk] of, in voorkomend geval, op het tijdstip bepaald in de vordering” moet worden verleend.

2.4. De regeling van de inkijkoperatie wordt aangepast. Zo wordt het mogelijk gesloten voorwerpen die op de betreden plaats te vinden zijn, te openen en voorwerpen voor een beperkte duur mee te nemen wanneer het onderzoek van het voorwerp niet ter plaatse kan gebeuren en de informatie niet op een andere manier kan worden verkregen. Ook wordt de inkijkoperatie ten aanzien van informaticasystemen mogelijk gemaakt. Deze laatste bevoegdheid wordt voorbehouden aan de onderzoeksrechter.

2.5. Er worden nieuwe bepalingen ingevoerd die het mogelijk maken dat de procureur des Konings bepaalde politiediensten machtigt op het internet, desnoods onder een fictieve naam, contact te onderhouden met een of meer personen waartegen ernstige aanwijzingen bestaan dat zij misdrijven plegen die gestraft worden met een gevangenisstraf van een jaar of meer. Alle in het raam hiervan genomen contacten moeten worden geregistreerd. Mits machtiging van de procureur des Konings kunnen in het raam van deze opdracht strikt noodzakelijke strafbare feiten gepleegd worden door politieambtenaren.

2.6. De termijn voor observatie bedoeld in artikel 47*sexies* van het Wetboek van Strafvordering, die thans één maand bedraagt maar kan worden verlengd, wordt op drie maanden gebracht, eveneens verlengbaar.

2.7. De maximum gevangenisstraf voor de niet-medewerking of het verhinderen van de zoeking in het informaticasysteem of de uitbreiding ervan, wordt opgetrokken van een tot drie jaar.

2.8. Artikel 90*ter* van het Wetboek van Strafvordering wordt grondig herschreven. Ten eerste kan de onderzoeksrechter in uitzonderlijke gevallen met een heimelijk oogmerk niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem of een deel ervan met technische hulpmiddelen laten onderscheppen, er kennis van nemen, doorzoeken en opnemen of een zoeking in een informaticasysteem of in een deel ervan uitbreiden. Ten tweede wordt de lijst uitgebreid van misdrijven waarvoor die maatregel mogelijk is.

2.9. Ook de artikelen 90*quater*, 90*quinquies*, 90*sexies* en 90*septies* van het Wetboek van Strafvordering worden herschreven teneinde onder meer de erin vervatte regelingen inzake beroepsgeheim en termijnen te verduidelijken.

2.10. Een aantal bepalingen van het Strafwetboek worden aangepast aan de nieuwe terminologie die wordt gehanteerd in artikel 90*ter* van het Wetboek van Strafvordering.

2.11. Tot slot wordt een gegevensbank van stemafdrukken geïntegreerd in de Algemene Nationale Gegevensbank bedoeld in de wet van 5 augustus 1992 “op het politieambt” teneinde de identificatie te vergemakkelijken van personen die

un certain nombre d’exigences procédurales. Il est en outre précisé que le concours ordonné doit être prêté “en temps réel [lire vraisemblablement: immédiatement] ou, le cas échéant, au moment précisé dans la réquisition”.

2.4. La réglementation du contrôle visuel discret est adaptée. Il devient ainsi possible d’ouvrir des objets fermés se trouvant sur les lieux visités, et d’empor*ter* des objets pour une durée limitée si leur examen ne peut se faire sur place et si l’information ne peut être obtenue d’une autre manière. Le contrôle visuel discret dans un système informatique est également rendu possible. Ce pouvoir est cependant réservé au juge d’instruction.

2.5. De nouvelles dispositions sont prévues, lesquelles habilitent le procureur de Roi à autoriser certains services de police à entretenir, le cas échéant sous une identité fictive, des contacts sur internet avec une ou plusieurs personnes concernant lesquelles il existe des indices sérieux qu’elles commettent des infractions pouvant donner lieu à un emprisonnement d’un an ou plus. Tous les contacts pris dans ce cadre doivent être enregistrés. Moyennant l’accord du procureur du Roi, les fonctionnaires de police peuvent, dans le cadre de cette mission, commettre des infractions strictement nécessaires.

2.6. La période au cours de laquelle l’observation peut être exécutée, visée à l’article 47*sexies* du Code d’instruction criminelle, qui est actuellement fixée à un mois, mais peut être prolongée, est portée à trois mois, également prolongeable.

2.7. La peine d’emprisonnement maximale pour refus de collaboration ou entrave à la recherche dans le système informatique ou à son extension est portée d’un an à trois ans.

2.8. L’article 90*ter* du Code d’instruction criminelle est remanié en profondeur. En premier lieu, le juge d’instruction peut, dans des cas exceptionnels, dans un but secret, faire intercepter, prendre connaissance, explorer et enregistrer, à l’aide de moyens techniques, des communications non accessibles au public ou des données d’un système informatique ou d’une partie de celui-ci, ou étendre une recherche dans un système informatique ou une partie de celui-ci. En deuxième lieu, la liste des infractions qui peuvent justifier cette mesure est étendue.

2.9. Les articles 90*quater*, 90*quinquies*, 90*sexies* et 90*septies* du Code d’instruction criminelle sont également remaniés afin, notamment, de préciser les règles qui y sont énoncées en matière de secret professionnel et de délais.

2.10. Un certain nombre de dispositions du Code d’instruction criminelle sont adaptées à la nouvelle terminologie utilisée à l’article 90*ter* du Code d’instruction criminelle.

2.11. Enfin, une banque de données des empreintes vocales est intégrée dans la Banque de données Nationale Générale visée dans la loi du 5 août 1992 “sur la fonction de police”, afin de faciliter l’identification des personnes qui font

het voorwerp uitmaken of hebben uitgemaakt van afluisterdossiers uitgevoerd op verzoek van de gerechtelijke overheden.

VORMVEREISTEN

3. Over het ontwerp werd de Commissie voor de bescherming van de persoonlijke levenssfeer om advies gevraagd. Uit ingewonnen inlichtingen blijkt dat dit advies niet voor 18 mei 2016 zal worden verleend.

Om te vermijden dat de Raad van State advies moet verlenen over een niet-definitieve ontwerptekst en opdat hij met volledige kennis van zaken zijn advies zou kunnen uitbrengen, verdient het aanbeveling een voorontwerp van wet slechts aan de Raad van State voor te leggen nadat het alle achtereenvolgende stadia van de administratieve voorbereiding heeft doorgemaakt.[6]

Nu dat niet is gebeurd, moet de Raad van State erop wijzen dat, indien de voorgelegde tekst ten gevolge van het advies van die commissie nog wijzigingen zou ondergaan, de gewijzigde of toegevoegde bepalingen, ter inachtneming van het voorschrift van artikel 3, § 1, eerste lid, van de wetten op de Raad van State, alsnog aan de afdeling Wetgeving moeten worden voorgelegd.

ALGEMENE OPMERKINGEN

I. De internationale aspecten van computercriminaliteit

4.1. Door de hoge vlucht die de informaticatechnologie heeft genomen en de ongekende mogelijkheden die ze biedt, is ze een uitgelezen middel geworden voor het plegen van misdrijven. Dergelijke misdrijven in "*cyberspace*" (de virtuele wereld van computers) worden meestal aangeduid met de term "cybercriminaliteit" (*cybercrime*).

De lokalisering van dergelijke misdrijven is zeer moeilijk doordat de computernetwerken die het (decentraal georganiseerde) internet vormen niet aan landsgrenzen gebonden zijn. De constitutieve bestanddelen van een strafbaar feit kunnen op het grondgebied van verschillende staten gelokaliseerd zijn terwijl het soms zelfs niet duidelijk is waar ze gelokaliseerd zijn, en ze kunnen elkaar zeer snel opvolgen. De territoriale aanknopingspunten en de traditionele rechtshulpmechanismen zijn dan ook niet altijd adequaat om cybercriminaliteit doeltreffend te vervolgen en te bestraffen. Daardoor ontstaat de neiging om brede lokalisatiecriteria te gebruiken en ruime onderzoeksbevoegdheden te hanteren.

4.2. Over de lokalisering van misdrijven en het toekennen van opsporings- en vervolgingsbevoegdheden wordt door elk land, door middel van wetgeving of rechtspraak, in beginsel op unilaterale wijze beslist. Een van de fundamentele regels van het internationaal recht bepaalt echter dat een staat

[6] Zulks klemt des te meer wanneer het, zoals in dit geval, gaat om ontwerpen met belangrijke technische aspecten of implicaties waaromtrent de meer gespecialiseerde adviesorganen over een grotere feitelijke kennis beschikken dan de Raad van State.

ou ont fait l'objet de dossiers d'écoute réalisés à la demande des autorités judiciaires.

FORMALITÉS

3. La Commission de la protection de la vie privée a été saisie d'une demande d'avis sur le projet. Il ressort des informations recueillies que cet avis ne sera pas donné avant le 18 mai 2016.

Afin d'éviter que le Conseil d'État doive donner un avis sur un projet de texte qui n'est pas définitif et pour qu'il puisse donner un avis en pleine connaissance de cause, il est recommandé de ne soumettre un avant-projet de loi au Conseil d'État qu'à l'issue des différentes étapes de sa préparation administrative [6].

Dès lors que tel n'a pas été le cas, le Conseil d'État se doit d'observer que, si le texte à l'examen devait encore subir des modifications consécutivement à l'avis de cette commission, il y aurait lieu, conformément au prescrit de l'article 3, § 1er, alinéa 1er, des lois sur le Conseil d'État, d'encore soumettre les dispositions modifiées ou nouvelles à la section de législation.

OBSERVATIONS GÉNÉRALES

I. Les aspects internationaux de la criminalité informatique

4.1. L'essor que la technologie informatique a connu et les possibilités insoupçonnées qu'elle offre en ont fait un moyen idéal pour commettre des infractions. De telles infractions dans le "cyberespace" (le monde virtuel des ordinateurs) sont généralement désignées par le terme "cybercriminalité" (cybercrime).

La localisation de telles infractions est très difficile, les réseaux d'ordinateurs qui constituent l'internet (organisé d'une manière décentralisée) ne connaissant pas de frontières étatiques. Les éléments constitutifs d'une infraction peuvent être localisés sur le territoire de plusieurs États, alors que leur localisation est même parfois difficile à déterminer, et ils peuvent se succéder très rapidement. Les critères de rattachement territorial et les mécanismes traditionnels d'entraide judiciaire ne sont dès lors pas toujours adéquats pour poursuivre et sanctionner efficacement la cybercriminalité. Il s'ensuit une tendance à utiliser des critères de localisation larges et des pouvoirs d'enquête étendus.

4.2. Chaque pays prend en principe unilatéralement, par voie législative ou jurisprudentielle, des mesures concernant de la localisation des infractions et l'attribution des pouvoirs de recherche et de poursuite. Une des règles fondamentales du droit international exige cependant qu'un État exerce l'autorité

[6] Cela d'autant plus vrai que, comme en l'espèce, il s'agit de projets qui présentent d'importants aspects techniques ou qui ont des implications pour lesquels les organes consultatifs plus spécialisés disposent d'une plus grande expertise que le Conseil d'État.

staatsgezag uitoefent op zijn eigen grondgebied, en dat alleen doet, zonder inmenging van enige andere staat. Gelet op dit *territorialiteitsbeginsel* is elke extraterritorialiteit inzake opsporing en vervolging in wezen problematisch omdat het tot een conflict met het staatsgezag van een andere staat of andere staten kan leiden.

De Belgische strafwet bepaalt dat de Belgische autoriteiten de daders van in België gepleegde misdrijven, ongeacht of zij Belg of vreemdeling zijn, kunnen opsporen, vervolgen en bestraffen (artikel 3 van het Strafwetboek). Het Hof van Cassatie heeft van zijn kant geoordeeld dat een misdrijf in België gepleegd is, als een van de constitutieve bestanddelen ervan er gelokaliseerd is.[7] Dezelfde autoriteiten mogen daarentegen de dader van een in het buitenland gepleegd misdrijf, ongeacht of hij Belg of vreemdeling is, niet vervolgen of straffen dan in de gevallen bij de wet bepaald (artikel 4 van het Strafwetboek).

Het Hof van Cassatie heeft erop gewezen dat een staat enkel op zijn eigen grondgebied dwangmaatregelen kan nemen om de naleving van zijn wetten af te dwingen en dat hij zich, zo hij een dergelijke maatregel neemt op het grondgebied van een andere staat, een extraterritoriale rechtsmacht toekent die de soevereiniteit van die staat miskent.[8]

Het is echter niet eenvoudig de precieze draagwijdte van het territorialiteitsbeginsel te bepalen ten aanzien van het optreden van justitie of politie in verband met informaticagegevens, inzonderheid wat betreft bevelen tot opsporing en

étatique sur son propre territoire, et qu'il le fasse seul, sans immixtion d'aucun autre État. Eu égard à ce principe de territorialité, toute extraterritorialité en matière de recherche et de poursuite est fondamentalement problématique, dès lors qu'elle peut entraîner un conflit avec la souveraineté d'un ou de plusieurs autres États.

Le droit pénal belge dispose que les autorités belges peuvent rechercher, poursuivre et sanctionner les auteurs d'infractions commises en Belgique, qu'ils soient belges ou étrangers (article 3 du Code pénal). Pour sa part, la Cour de cassation a jugé qu'une infraction est commise en Belgique si l'un de ses éléments constitutifs y est localisé [7]. Par contre, les mêmes autorités ne peuvent poursuivre ou punir l'auteur, belge ou étranger, d'une infraction commise à l'étranger, que dans les cas déterminés par la loi (article 4 du Code pénal).

La Cour de cassation a souligné qu'un État ne peut prendre des mesures coercitives pour assurer le respect de ses lois que sur son propre territoire et que, s'il prend une telle mesure sur le territoire d'un autre État, il s'attribue une juridiction extraterritoriale, méconnaissant ainsi la souveraineté de cet État [8].

Il n'est cependant pas aisé de déterminer la portée exacte du principe de territorialité quant aux actions de la justice ou de la police touchant à des données informatiques, notamment, les mandats de perquisition et de saisie qui concernent de

7 Zie o.a.: Cass. 23 januari 1979, *Arr.Cass.* 1979, 575, en *Pas.* 1979, I, 582; Cass. 4 februari 1986, *Arr.Cass.* 1985-86, 765, nr. 355, en *Pas.* 1986, I, 671, nr. 355; Cass. 21 juni 1989, *Arr.Cass.* 1988-89, 1272, nr. 620, en *Pas.* 1989, I, 1162, nr. 620.

8 Een staat neemt een dwangmaatregel op zijn eigen grondgebied wanneer er tussen die maatregel en dat grondgebied een voldoende territoriaal aanknopingspunt bestaat – welk territoriaal aanknopingspunt minstens vereist is, wordt onder meer bepaald door de aard en de draagwijdte van de dwangmaatregel (Cass. 1 december 2015, *RABG* 2016, 485, noot K. De Schepper).

7 Voir notamment: Cass. 23 janvier 1979, *Pas.* 1979, I, 582 et *Arr. Cass.* 1979, 575; Cass., 4 février 1986, *Pas.*, I, 671, n° 355 et *Arr. Cass.* 1985-86, 765, n° 355; Cass. 21 juin 1989, *Pas.* 1989, I, 1162, n° 620 et *Arr. Cass.* 1988-89, 1272, n° 620.

8 Un État prend une mesure coercitive sur son propre territoire lorsqu'il existe entre cette mesure et ce territoire un lien de rattachement territorial suffisant – le lien de rattachement minimal requis est notamment déterminé par la nature et la portée de la mesure coercitive (Cass. 1er décembre 2015, *RAGB* 2016, 485, note K. De Schepper).

inbeslagneming van zulke gegevens.[9] Dat probleem is het gevolg van de blijvende onzekerheid die soms bestaat over de vraag waar informaticagegevens precies te vinden zijn, maar het houdt ook verband met het gegeven dat een autoriteit door middel van virtuele opsporingshandelingen gegevens in het buitenland kan navorsen zonder daarom het grondgebied van de staat waaronder ze ressorteert, fysiek te verlaten.[10]

Het standpunt dat om een onderzoek wettig te laten verlopen, het noodzakelijk is dat de data zich niet op het grondgebied van een vreemde staat bevinden, is uiteengezet in een "explanatory memorandum" bij aanbeveling nr. R (95) 13 van het Comité van ministers van de Raad van Europa van 11 september 1995. In die toelichting staat te lezen dat wat betreft "*data stored in another country (...), [m]ost member states tend to consider such a transborder network search by investigating authorities, without the consent of the competent authorities of the country concerned, as a possible violation of state sovereignty and of international law and, partially, also as a circumvention of the traditional path of mutual legal assistanc*e".[11]

4.3. Met de wet van 28 november 2000 "inzake informaticacriminaliteit" heeft de Belgische wetgever ter zake een hele reeks vernieuwingen doorgevoerd in het Strafwetboek

telles données [9]. La difficulté ne résulte pas seulement de l'incertitude persistante qui peut parfois planer sur la question de savoir où sont exactement localisées ces données informatiques, mais tient également au fait que, grâce à des opérations de recherche virtuelles, une autorité est capable, sans pour autant quitter physiquement le territoire de l'État dont elle relève, d'investiguer sur des données situées à l'étranger [10].

L'opinion selon laquelle la licéité d'une enquête requiert que les données ne se trouvent pas localisées sur le territoire d'un État étranger a été exposée dans un rapport explicatif de la recommandation n° R(95) 13 du Comité des ministres du Conseil de l'Europe du 11 septembre 1995. Dans ce rapport, on peut lire qu'à l'égard "des données stockées dans un autre pays (...), [l]a plupart des États membres tendent à considérer qu'une perquisition transfrontalière sur réseau menée par les autorités chargées de l'enquête sans l'autorisation des autorités compétentes du pays concerné pourrait constituer une violation de la souveraineté de l'État et du droit international, ainsi qu'un contournement partiel de la voie traditionnelle d'entraide judiciaire" [11].

4.3. En adoptant la loi du 28 novembre 2000 "relative à la criminalité informatique", le législateur belge a introduit dans le Code pénal et dans le Code d'instruction criminelle toute une

---

9 Zie o.m.: K. De Schepper en F. Verbruggen, "Ontnappen *space invaders* aan onze *pacmannen*? De materiële en formele strafrechtsmacht van België bij strafbare weigering van medewerking door elektronische dienstverleners", *T.Strafr.* 2013, 143-166; B.-J. Koops en M. Goodwin, *Cyberspace, the cloud, and cross-border criminal investigation. The limits and possibilities of international law*, 2014, http://english.eu2016.nl/binaries/eu2016-en/documents/publications/2016/03/7/c-koops-goodwin-cross-border-criminal-investigation/c-koops-goodwin-cross-border-criminal-investigation.pdf; A.-M. Osula, *Accessing Extraterritorially Located Data: Options for States*, 2015, *http://english.eu2016.nl/binaries/eu2016-en/documents/publications/2016/03/7/c-osula-accessing-extraterritorially-located-data-options-for-states_anna-maria_osula/c-osula-accessing-extraterritorially-located-data-options-for-states-anna-maria-osula.pdf*; A. Woods, *Data beyond borders. Mutual Legal assistance in the internet age*, 2015, https://globalnetworkinitiative.org/sites/default/files/GNI %20MLAT %20Report.pdf; M. Zoetekouw, *Ignorantia Terrae Non Excusat. A discussion paper regarding the locality of enforcement*, 2016, http://english.eu2016.nl/binaries/eu2016-en/documents/publications/2016/03/7/c-mzoetekouw---ignorantia-terrae-non-excusat---discussion-paper-for-the-crossing-borders---jurisdiction-in-cyberspace-conference-march-2016-final/c-mzoetekouw-ignorantia-terrae-non-excusat-discussion-paper-for-the-crossing-borders-jurisdiction-in-cyberspace-conference-march-2016-final.pdf.

10 Over de lokalisering van virtuele opsporingshandelingen, zie: C. Conings, "De lokalisatie van opsporing in een virtuele omgeving. Wie zoekt waar in cyberspace?", *NC* 2014, 1-25.

11 Explanatory memorandum on recommendation N° R (95) 13 of the Committee of ministers to member states concerning problems of criminal procedural law connected with information technology, aangenomen door het Comité van ministers op 11 september 1995, *https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804e4602*.

9 Voir notamment: K. De Schepper et F. Verbruggen, "Ontnappen *space invaders* aan onze *pacmannen*? De materiële en formele strafrechtsmacht van België bij strafbare weigering van medewerking door elektronische dienstverleners", *T. Strafr.* 2013, 143-166; B.-J. Koops et M. Goodwin, *Cyberspace, the cloud, and cross-border criminal investigation. The limits and possibilities of international law*, 2014, http://english.eu2016.nl/binaries/eu2016-en/documents/publications/2016/03/7/c-koops-goodwin-cross-border-criminal-investigation/c-koops-goodwin-cross-border-criminal-investigation.pdf; A.-M. Osula, *Accessing Extraterritorially Located Data: Options for States*, 2015, *http://english.eu2016.nl/binaries/eu2016-en/documents/publications/2016/03/7/c-osula-accessing-extraterritorially-located-data-options-for-states_anna-maria_osula/c-osula-accessing-extraterritorially-located-data-options-for-states-anna-maria-osula.pdf*; A. Woods, *Data beyond borders. Mutual Legal assistance in the internet age*, 2015, https://globalnetworkinitiative.org/sites/default/files/GNI %20MLAT %20Report.pdf; M. Zoetekouw, *Ignorantia Terrae Non Excusat. A discussion paper regarding the locality of enforcement*, 2016, *http://english.eu2016.nl/binaries/eu2016-en/documents/publications/2016/03/7/c-mzoetekouw---ignorantia-terrae-non-excusat---discussion-paper-for-the-crossing-borders---jurisdiction-in-cyberspace-conference-march-2016-final/c-mzoetekouw-ignorantia-terrae-non-excusat-discussion-paper-for-the-crossing-borders-jurisdiction-in-cyberspace-conference-march-2016-final.pdf*.

10 En ce qui concerne la localisation d'opérations de recherche virtuelles, voir C. Conings, "De lokalisatie van opsporing in een virtuele omgeving. Wie zoekt waar in cyberspace?", *NC* 2014, 1-25.

11 Rapport explicatif de la ecommandation N° R(95) 13 du Comité des ministres aux États membres relative aux problèmes de procédure pénale liés à la technologie de l'information, adoptée par le Comité des ministres le 11 septembre 1995, *https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804e15f8*.

en in het Wetboek van Strafvordering,[12] in het bijzonder door het invoeren van de mogelijkheid om door middel van een zoeking in een informaticasysteem of in een deel ervan bewijsmateriaal in het buitenland te bekomen (artikel 88*ter* van het Wetboek van Strafvordering).[13] De memorie bij het ontwerp dat tot die wet heeft geleid, bevat in dit verband onder meer de volgende toelichting:

"De internationale verwevenheid van de netwerken zal wellicht onvermijdelijk aanleiding geven tot gevallen, waar tijdens de netwerkzoeking bestanden worden bevraagd of zouden moeten worden geconsulteerd die zich, zonder dat de gerechtelijke diensten zich dit tijdig realiseren, in het buitenland zijn gesitueerd. De mogelijkheden om als zodanig doelbewust de zoeking uit te breiden naar systemen die in het buitenland zijn gesitueerd, roepen in de huidige stand van het internationale publiekrecht een aantal juridische vragen op. De bevoegdheden waarover de overheid beschikt om onderzoekshandelingen te stellen in het kader van een strafprocedure kunnen immers in principe enkel worden uitgeoefend op het nationale territorium waarover die overheid gezag heeft. Dit houdt ongetwijfeld verband met het feit dat het strafrecht zeer sterk verbonden is met de notie van staatssoevereiniteit. Het hangt eveneens samen met het beginsel van de goede trouw in de interstatelijke betrekkingen. Tegelijk komt de klassieke invulling van het concept soevereiniteit in deze context onder druk te staan, enerzijds omwille van de toenemende internationalisering van de financieel-economische criminaliteit, en anderzijds door de enorme vlucht die de informatietechnologie heeft genomen. Men is er zich meer en meer van bewust dat de traditionele vormen van internationale gerechtelijke samenwerking, die juist in het leven werden geroepen om aan de beperkingen van de nationale opsporings- en onderzoeksbevoegdheden te remediëren, niet enkel moeten worden gemoderniseerd, maar op sommige punten moeten worden geïnnoveerd. Vandaar dat thans met name inzake opsporingen en onderzoek in een IT-context op internationaal vlak naar oplossingen wordt gezocht in diverse fora (Europese Unie, Raad van Europa, blz. 8).

Het huidige ontwerp kan derhalve niet eenzijdig oplossingen aanreiken voor alle vragen die kunnen rijzen inzake de internationale netwerkzoeking. Een aantal punten zullen onmiskenbaar via internationale instrumenten of overleg met andere staten moeten worden behandeld. Dit neemt evenwel niet weg dat de problemen vandaag bestaan, en dat derhalve een juridisch houvast moet worden geboden aan de mensen die op het terrein naar aanleiding van een zoeking in een computersysteem met de problematiek van op internationale schaal verbonden informaticasystemen worden geconfronteerd. Er moet immers een antwoord geboden worden aan de noden van een effectieve criminaliteitsbestrijding op de informatiesnelwegen.

[12] Over de wet van 28 november 2000, zie o.m.: S. Evrard, "La loi du 28 november 2000 relative à la criminalité informatique", *JT* 2001, 241-245; C. Meunier, "La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique", *Rev.dr.pén.* 2001, 611-690.

[13] Over de huidige wettelijke regeling inzake cybercrime, zie: J. Kerkhofs en P. Van Linthout, *Cybercrime*, Brussel, Politeia, 2013.

série d'innovations en la matière [12], en prévoyant notamment la possibilité de recueillir des preuves à l'étranger par la voie d'une recherche dans un système informatique ou une partie de celui-ci (article 88*ter* du Code d'instruction criminelle) [13]. À cet égard, l'exposé des motifs du projet à l'origine de cette loi, comporte notamment les précisions suivantes:

"Le caractère international des réseaux engendrera inévitablement des situations dans lesquelles, lors de la recherche sur réseau, des fichiers seront ou devront être consultés avant même que les services judiciaires n'aient le temps de réaliser que ces fichiers proviennent de l'étranger. Les possibilités d'étendre de manière consciente la recherche à des systèmes se trouvant à l'étranger suscitent un certain nombre de questions juridiques compte tenu de l'état actuel du droit public international. La compétence des autorités de poser des actes d'instruction dans le cadre d'une procédure pénale ne peut être exercée, en principe, que sur le territoire national placé sous leur autorité. Ceci est certainement dû au fait que le droit pénal est étroitement lié avec les principes de souveraineté nationale et de bonne foi dans les relations interétatiques. De même, l'interprétation classique du concept de souveraineté est influencée par l'internationalisation sans cesse croissante de la criminalité économico-financière, d'une part, et par la rapidité avec laquelle la technologie de l'information évolue, d'autre part. On est de plus en plus conscient du fait qu'il est nécessaire de moderniser et, sur certains points, d'innover les formes traditionnelles d'entraide judiciaire internationale mises en place justement pour pallier les lacunes sur le plan des compétences en matière d'information et d'instruction au niveau national. D'où la raison d'organiser différents forums pour appor*ter* la solution aux problèmes rencontrés, dans le contexte de la technologie de l'information, en matière d'instruction et d'information au niveau international (Union européenne, Conseil de l'Europe, p. 8).

Par conséquent, le présent projet n'offre pas de réponses unilatérales à toutes les questions qui peuvent se poser en matière de recherche internationale sur réseau. Un certain nombre de points devront indéniablement être traités à l'aide d'instruments internationaux ou en concertation avec d'autres États. Néanmoins, les problèmes se posent aujourd'hui et il est dès lors indispensable d'offrir des points d'appui juridiques aux personnes qui, à la suite d'une recherche dans un système informatique, sont confrontées sur le terrain à la problématique des systèmes informatiques en réseau. Il convient de répondre de manière satisfaisante aux besoins en matière de lutte contre la criminalité sur les autoroutes de l'information.

[12] Au sujet de la loi du 28 novembre 2000, voir notamment: S. Evrard, "La loi du 28 novembre 2000 relative à la criminalité informatique", *JT* 2001, 241-245; C. Meunier, "La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique", *Rev. dr. pén.*, 2001, 611-690.

[13] En ce qui concerne le dispositif législatif actuel en matière de cybercriminalité, voir: J. Kerkhofs et P. Van Linthout, *Cybercrime*, Bruxelles, Politeia, 2013.

Daarom wordt in dit ontwerp in deze materie een voorzichtige, maar pragmatische positie ingenomen. Het is duidelijk dat de grensoverschrijdende zoeking niet als regel kan worden gesteld. Er kunnen immers ernstige problemen rijzen, wanneer de gerechtelijke overheden van een staat eenzijdig en welbewust een netwerkzoeking uitbreiden naar het buitenland zonder de bevoegde buitenlandse autoriteiten hierin te kennen. Wanneer derhalve voldoende tijd en kennis voorhanden is, moet de weg van de klassieke internationale rogatoire commissies worden gevolgd, bij ontstentenis van juridisch adequate alternatieven op dit ogenblik.

De wijze waarop computers, evenals de verbindingen daartussen, functioneren, kan zeer complex zijn. Daardoor zijn er situaties denkbaar waar tijdens een zoeking in een computersysteem data worden bekomen die niet zijn opgeslagen op de plaats waar de zoeking plaatsvindt (elders in het land of in het buitenland), maar waar de speurders zich hiervan niet bewust zijn of er niet in slagen de exacte lokatie van de data te bepalen.

Wanneer per toeval of onopzettelijk data uit het buitenland worden bekomen, staat de rechtmatigheid van het strafprocessueel optreden van de overheid niet principieel ter discussie en is er derhalve geen aanleiding om de bekomen gegevens internrechtelijk *a priori* als bewijsmateriaal uit te sluiten. Nadat is vastgesteld dat de data in het buitenland werden bekomen, is het evenwel in het kader van goede interstatelijke betrekkingen aangewezen contact te nemen met de overheid van de andere betrokken staat waar de data gelokaliseerd zijn, als deze redelijkerwijze kan worden bepaald, teneinde deze staat toe te laten een standpunt ter zake in te nemen.

Ingeval de speurders tijdens de zoeking wel kennis hebben van het feit dat de gezochte bestanden in het buitenland gesitueerd zijn, maar er redelijkerwijze niet in slagen de betrokken staat te identificeren, wordt dezelfde oplossing als hiervoor vermeld weerhouden, aangezien ook internationaal overleg deze situatie niet kan oplossen.

Daarnaast moet tegelijk vastgesteld worden dat een impasse dreigt te ontstaan, omdat de logica die geldt voor een louter nationale uitbreiding van een zoeking in een informaticasysteem, onverkort en misschien nog sterker geldt in een “global village”. Het belang om in dringende gevallen de teloorgang van computerbestanden te vrijwaren voor de bewijsvoering botst hier op de thans nog algemeen verspreide traditionele invulling van het concept soevereiniteit. Men denke hier bijvoorbeeld aan het geval waar tijdens de zoeking wordt vastgesteld dat de relevante files zich op een welbepaalde plaats in het buitenland bevinden. Het stopzetten van de zoeking en het instellen van een internationale rogatoire commissie om ter plekke een huiszoeking te laten uitvoeren biedt de betrokkenen alle mogelijkheden om via de telecommunicatiekanalen ondertussen de data zelf te laten verdwijnen.

Vandaar de nood om in spoedeisende gevallen, naar analogie met de regelingen inzake “*hot pursuit*” over te kunnen gaan tot het nemen van voorlopige maatregelen om de teloorgang van het bewijsmateriaal te vrijwaren (kopiëren, maar niet blokkeren van de data). Het belang van de

C’est pour cette raison qu’a été adoptée, dans le présent projet, une attitude prudente mais pragmatique en la matière. Il est clair que les recherches effectuées en dehors des frontières doivent rester exceptionnelles. Des problèmes peuvent néanmoins surgir lorsque les autorités judiciaires d’un État étendent unilatéralement et consciemment leurs recherches sur réseau à l’étranger sans en informer les autorités étrangères compétentes. Si le temps et les connaissances le permettent, et à défaut de solutions alternatives adéquates sur le plan juridique à l’heure actuelle, il convient de suivre la procédure classique des commissions rogatoires internationales.

Le mode de fonctionnement ainsi que les connexions des ordinateurs peuvent être très complexes. C’est pourquoi on peut envisager des situations dans lesquelles il est possible, lors d’une recherche dans un système informatique, d’obtenir des données qui ne sont pas stockées à l’endroit où s’effectue la recherche (c’est-à-dire ailleurs dans le pays ou à l’étranger), et dont les enquêteurs ignorent l’existence ou ne parviennent pas à localiser l’origine avec exactitude.

Lorsque des données sont recueillies à l’étranger par hasard ou involontairement, le bien-fondé de l’action pénale menée par les autorités ne peut en principe pas être mis en doute et il n’y a donc aucune raison d’exclure *a priori* les données recueillies par voie intrajudiciaire comme étant des éléments de preuve. Après qu’il a été constaté que les données ont été recueillies à l’étranger, il est indiqué de contacter les autorités du pays dans lequel les données ont été localisées, du moins si celui-ci peut être déterminé avec précision, afin de maintenir de bonnes relations interétatiques et permettre à ce pays d’adopter un point de vue à ce propos.

Lorsque les enquêteurs apprennent, au cours des recherches, que les fichiers recherchés se trouvent à l’étranger et qu’ils ne parviennent pas à identifier le pays concerné avec certitude, on opte pour la solution déjà mentionnée précédemment étant donné qu’aucune concertation internationale n’est à même d’appor*ter* une solution à cette situation.

De plus, il faut également préciser que l’on risque d’aboutir sur une impasse parce que la logique sur laquelle repose une extension purement nationale d’une recherche dans un système informatique s’applique également de manière intégrale et peut-être encore plus intensivement au “global village”. Dans ces cas urgents, l’intérêt de préserver des fichiers informatiques pouvant servir d’éléments de preuve entre en conflit avec le concept traditionnel de souveraineté encore très largement répandu à l’heure actuelle. On pense, par exemple, au cas dans lequel il est établi, au cours des recherches, que le fichier pertinent se trouve à l’étranger dans un endroit bien déterminé. L’arrêt des recherches et la mise sur pied d’une commission rogatoire internationale en vue d’effectuer une perquisition sur place laisse aux intéressés suffisamment de temps pour faire disparaître les données via les canaux de télécommunication.

D’où la nécessité, dans des cas urgents, d’agir par analogie aux règles en matière de “*hot pursuit*”, c’est- à-dire de pouvoir prendre des mesures destinées à empêcher la disparition des éléments de preuve (en copiant les données et non en les bloquant). L’importance de la vérité dans des cas

waarheidsvinding in gevallen van ernstige criminaliteit kan een dergelijke grensoverschrijdende zoeking uitzonderlijk rechtvaardigen. In dergelijke gevallen is het evenwel onontbeerlijk om de betrokken andere staat te informeren teneinde deze toe te laten na te gaan of al dan niet een inbreuk op de rechtsorde werd gemaakt. Internationaalrechtelijk kan hierbij onder andere het element reciprociteit een rol spelen. Op deze wijze is, los van een verdragsrechtelijke basis, een vorm van wederzijdse steun mogelijk, die van geval tot geval voor alle betrokken staten nuttig kan zijn. Niettemin is het in het bijzonder betreffende dergelijke situaties dat in de huidige stand van het internationaal publiekrecht geen klare invulling bestaat van wat de draagwijdte van het concept soevereiniteit in de "cyberruimte" nog kan zijn.

In de voormelde gevallen vereist een optreden "te goeder trouw" ten aanzien van andere staten, evenals de zorg voor het vrijwaren van de rechtmatigheid van het bewijs dat door de gerechtelijke overheden redelijke inspanningen worden gedaan om de data zo exact mogelijk te lokaliseren. Aldus wordt eveneens vermeden dat men het verwijt zou kunnen opperen dat de opsporingsdiensten nalatig geweest zijn om inbreuken op de rechtsorde van andere staten te vermijden."[14]

4.4. Toen de wetgever de wet van 28 november 2000 aannam, was er nog geen enkele internationale regeling inzake de netwerkzoeking. Een dergelijke regeling is in 2001 voor het eerst tot stand gekomen met het Cybercrimeverdrag, dat in het raam van de Raad van Europa is uitgewerkt. Dit verdrag is in België op 1 december 2012 van toepassing geworden.

Het Cybercrimeverdrag bevat echter slechts een zeer beperkte regeling inzake het verwerven van data in het buitenland. Het gaat om artikel 32 van het verdrag, dat twee hypothesen inzake de grensoverschrijdende toegang tot opgeslagen informaticagegevens regelt, enerzijds, de toegang tot publiek toegankelijke gegevens en, anderzijds, de toegang mits instemming. Dat artikel luidt:

"Article 32. T*ransborder access to stored computer data with consent or where publicly available*

A Party may, without the authorisation of another Party:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

de grande criminalité justifie que de telles recherches soient menées à l'étranger exceptionnellement. Dans ces cas, il semble toutefois essentiel d'informer l'État concerné afin de permettre à celui-ci de vérifier si une infraction à l'ordre juridique a été commise ou non. D'un point de vue judiciaire et international, la réciprocité, par exemple, peut jouer un certain rôle. Ainsi, il est possible, indépendamment de toute convention sur le plan juridique, de mettre sur pied une forme d'appui réciproque qui, selon les cas, peut être utile à tous les États concernés. Toutefois, le droit public international ne donne, à l'heure actuelle, aucune interprétation précise quant à l'importance que peut avoir le concept de souveraineté dans le "cyberespace", surtout dans ce genre de situations.

Dans les cas précités, une action menée "de bonne foi" par un État dans d'autres pays ainsi que le souci de garantir le bien-fondé de la preuve exigent des efforts importants de la part des autorités judiciaires pour localiser les données autant que possible. Cela permettra également de reprocher aux services de recherches d'avoir été négligents et de pas avoir été capables d'empêcher la perpétration des infractions à l'ordre juridique d'autres pays" [14].

4.4. À l'époque où le législateur a adopté la loi du 28 novembre 2000, il n'existait pas encore de règlement international en matière de recherche sur réseau. Pareil règlement a été instauré pour la première fois en 2001 avec la Convention sur la cybercriminalité, élaborée dans le cadre du Conseil de l'Europe. Cette convention est devenue applicable en Belgique le 1er décembre 2012.

Toutefois, la Convention sur la cybercriminalité ne contient qu'un dispositif très limité concernant l'acquisition de données à l'étranger. Il s'agit de l'article 32 de la convention, qui règle deux hypothèses en matière d'accès transfrontière à des données informatiques stockées, d'une part, l'accès à des données accessibles au public et, d'autre part, l'accès avec consentement. Cet article s'énonce comme suit:

"Article 32. Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public

Une Partie peut, sans l'autorisation d'une autre Partie:

a. accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; ou

14 *Parl.St.* Kamer, nrs. 50-0213/001 en 50-0214/001, 23-26.

14 *Doc. parl., Chambre*, nos 50-0213/001 et 50-0214/001, 23-26.

b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system."[15]

In het *Explanatory [Memorandum]* is bij dit artikel volgende toelichting gegeven:

"293. *The issue of when a Party is permitted to unilaterally access computer data stored in another Party without seeking mutual assistance was a question that the drafters of the Convention discussed at length. There was detailed consideration of instances in which it may be acceptable for States to act unilaterally and those in which it may not. The drafters ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. In part, this was due to a lack of concrete experience with such situations to date; and, in part, this was due to an understanding that the proper solution often turned on the precise circumstances of the individual case, thereby making it difficult to formulate general rules. Ultimately, the drafters decided to only set forth in Article 32 of the Convention situations in which all agreed that unilateral action is permissible. They agreed not to regulate other situations until such time as further experience has been gathered and further discussions may be held in light thereof. In this regard, Article 39, paragraph 3 provides that other situations are neither authorised, nor precluded.*

294. *Article 32 (Transborder access to stored computer data with consent or where publicly available) addresses two situations: first, where the data being accessed is publicly available, and second, where the Party has accessed or received data located outside of its territory through a computer system in its territory, and it has obtained the lawful and voluntary consent of the person who has lawful authority to disclose the data to the Party through that system. Who is a person that is "lawfully authorised" to disclose data may vary depending on the circumstances, the nature of the person and the applicable law concerned. For example, a person's e-mail may be stored in another country by a service provider, or a person may intentionally store data in another country.*

[15] Voor een grondige bespreking van dit verdragsartikel, zie: Cybercrime Convention Committee, *Transborder access and jurisdiction: What are the options?*, 6 december 2012, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8; Cybercrime Convention Committee, *Transborder access and jurisdiction: Transborder access to data and jurisdiction: Options for further action by the T-CY, 3 december 2014, http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY %282014 %2916_TBGroupReport_v17adopted.pdf*.

b. accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre État, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique" [15].

À propos de cet article, le rapport explicatif précise ce qui suit:

"293. La question de savoir quand une Partie est autorisée à accéder unilatéralement aux données informatiques stockées sur le territoire d'une autre Partie a été longuement examinée par les auteurs de la Convention. Ils ont passé en revue de façon détaillée les situations dans lesquelles il pourrait être acceptable que des États agissent de façon unilatérale et celles dans lesquelles tel n'est pas le cas. En définitive, les auteurs ont conclu qu'il n'était pas encore possible d'élaborer un régime global juridiquement contraignant applicable à ce domaine. C'était partiellement dû au fait que l'on ne dispose à ce jour d'aucun exemple concret; cela tenait également au fait que l'on considérait que la meilleure façon de trancher la question était souvent liée aux circonstances de chaque cas d'espèce, ce qui ne permettait guère de formuler des règles générales. Les auteurs ont fini par décider de ne faire figurer dans l'article 32 de la Convention que les situations dans lesquelles l'action unilatérale était unanimement considérée comme admissible. Ils sont convenus de ne réglementer aucune autre situation tant que l'on n'aurait pas recueilli de nouvelles données et poursuivi la discussion de la question. À cet égard, le paragraphe 3 de l'article 39 dispose que les autres situations ne sont ni autorisées ni exclues.

294. L'article 32 (Accès transfrontalier à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public) traite de deux situations: d'abord, celle dans laquelle les données en question sont accessibles au public, et ensuite celle dans laquelle la Partie a obtenu accès à ou reçu des données situées en dehors de son territoire, au moyen d'un système informatique situé sur son territoire, et a obtenu le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique. La question de savoir qui est la personne "légalement autorisée" pour communiquer des données peut varier en fonction des circonstances, la nature de la personne et du droit applicable concernés. Par

[15] Pour un commentaire approfondi de cet article de la convention, voir: *Cybercrime Convention Committee, Transborder access and jurisdiction: What are the options?,* 6 décembre 2012, *https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8*; *Cybercrime Convention Committee, Transborder access and jurisdiction: Transborder access to data and jurisdiction: Options for further action by the T-CY,* 3 décembre 2014, http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY %282014 %2916_TBGroupReport_v17adopted.pdf.

These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data, as provided in the Article."[16]

Het Cybercrimeverdrag is intussen van kracht in de meeste lidstaten van de Raad van Europa (evenwel niet in o.m. Griekenland, Ierland en Rusland), maar ook in niet-lidstaten zoals Australië, Canada, Japan, Panama en de Verenigde Staten.

Sedert 1 december 2012 moeten de betrokken bepalingen van het Wetboek van Strafvordering dus worden gelezen in samenhang met artikel 32 van het verdrag voor die activiteiten die erdoor worden geregeld.

4.5. Net als de huidige regeling (artikel 88*ter* van het Wetboek van Strafvordering), bevat ook het ontwerp bepalingen die het de Belgische autoriteiten mogelijk maken om een zoeking in een informaticasysteem (of in een deel ervan) uit te breiden naar een informaticasysteem (of naar een deel ervan) dat zich op "een andere plaats" bevindt dan waar de zoeking plaatsvindt (artikel 2 van het ontwerp – ontworpen artikel 39*bis*, § 4, van het Wetboek van Strafvordering). Daarmee wordt ook toegang verleend tot bewijsmaterieel dat niet in België gelokaliseerd kan worden.[17]

Ook de ontworpen bepalingen zullen moeten worden gelezen in samenhang met het Cybercrimeverdrag, vermits artikel 32 van het verdrag de mogelijkheden beperkt om een zoeking uit te breiden en die zoeking unilateraal te doen (d.w.z. zonder de rechtshulp van de andere staat of van andere staten in te roepen). Als het gaat om data die zich bijvoorbeeld in de Verenigde Staten bevinden, zal artikel 32 van het verdrag evenzeer moeten worden nageleefd. Gaat het evenwel om data die zich bevinden in een staat die geen partij bij het verdrag is of kunnen de data niet precies worden gelokaliseerd,[18] dan is het verdrag niet van toepassing, maar staat het optreden van de Belgische autoriteiten buiten de traditionele rechtshulpkanalen op gespannen voet met het territorialiteitsbeginsel.

II. Verruimde bevoegdheden van het openbaar ministerie in het licht van het eerbiedigen van de grondrechten

5. Een zoeking in een informaticasysteem kan een belangrijke inmenging vormen in het onder meer bij artikel 8 van het Europees Verdrag over de Rechten van de Mens en artikel 22 van de Grondwet gewaarborgde recht op eerbiediging

[16] Cybercrime Convention Committee, T-CY Guidance Note #3 Transborder access to data (Article 32), 3 december 2014, 4, *https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726a.*

[17] J. Kerkhofs en P. Van Linthout, *o.c.*, p. 268, nr. 281.

[18] In dat laatste geval wordt er blijkbaar doorgaans vanuit gegaan dat de zoeking op het eigen grondgebied plaatsheeft (M. Zoetekouw, *o.c*, 1).

exemple, le message électronique d'une personne peut être stocké dans un autre pays par un fournisseur de services ou une personne peut stocker délibérément des données dans un autre pays. Ces personnes peuvent récupérer les données et, pourvu qu'elles aient une autorité légale, elles peuvent les communiquer de leur propre gré aux agents chargés de l'application de la loi ou leur permettre d'accéder aux données, tel que prévu à l'article" [16].

Entre-temps, la Convention sur la cybercriminalité est entrée en vigueur dans la plupart des États membres du Conseil de l'Europe (mais pas, notamment, en Grèce, en Irlande et en Russie), et également dans des États non membres comme l'Australie, le Canada, le Japon, le Panama et les États-Unis.

Depuis le 1er décembre 2012, les dispositions concernées du Code d'instruction criminelle doivent donc être lues en combinaison avec l'article 32 de la convention pour les activités qu'il règle.

4.5. À l'instar du régime actuel (article 88*ter* du Code d'instruction criminelle), le projet comporte également des dispositions permettant aux autorités belges d'étendre une recherche dans un système informatique (ou une partie de celui-ci) vers un système informatique (ou une partie de celui-ci) qui se trouve "dans un autre lieu" que celui où la recherche est effectuée (article 2 du projet – article 39*bis*, § 4, en projet, du Code d'instruction criminelle). Ce faisant, on donne également accès à des éléments de preuve qui ne peuvent pas être localisés en Belgique [17].

Les dispositions en projet devront également être lues en combinaison avec la Convention sur la cybercriminalité, puisque l'article 32 de celle-ci limite les possibilités d'étendre une recherche et d'effectuer cette recherche unilatéralement (c'est-à-dire sans invoquer l'entraide judiciaire de l'autre État ou d'autres États). S'il s'agit de données se trouvant par exemple aux États-Unis, l'article 32 de la Convention devra tout autant être respecté. Toutefois, s'il s'agit de données se trouvant dans un État qui n'est pas partie à la Convention ou si les données ne peuvent pas être localisées avec précision [18], la convention ne sera alors pas d'application, mais l'intervention des autorités belges en dehors des canaux traditionnels d'entraide judiciaire se heurtera au principe de territorialité.

II. Compétences élargies du ministère public au regard du respect des droits fondamentaux

5. Une recherche dans un système informatique peut constituer une ingérence importante dans le droit au respect de la vie privée, garanti notamment par l'article 8 la Convention européenne des droits de l'Homme et par l'article 22 de la

[16] Cybercrime Convention Committee, T-CY Guidance Note #3 Transborder access to data (Article 32), 3 décembre 2014, 4, *https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726a.*

[17] J. Kerkhofs et P. Van Linthout, *o.c.,* p. 268, n° 281.

[18] Dans ce dernier cas, on semble généralement considérer que la recherche a lieu sur le propre territoire (M. Zoetekouw, *o.c.,* 1).

van het privéleven.[19] In het ontwerp worden ter zake belangrijke bevoegdheden overgeheveld van de onderzoeksrechter naar het openbaar ministerie. Al lijkt niet te worden vereist dat zulk een inmenging in het raam van het vooronderzoek steeds door een rechter wordt bevolen,[20] neemt dit element toch een belangrijke plaats in bij de proportionaliteitstoets die het Europees Hof voor de Rechten van de Mens[21] en het Grondwettelijk Hof[22] ter zake verrichten. Daarbij mag niet uit het oog worden verloren dat de onderzoeksrechter een onafhankelijk magistraat is die een objectief onderzoek voert, zowel *a charge* als *a décharge*, terwijl het openbaar ministerie partij in het strafproces is.[23] Het staat aan de wetgever, evenwel onder controle van de bevoegde rechtscolleges, met afweging van alle in het geding zijnde belangen[24] en rekening houdend met eerdere uitbreidingen van de bevoegdheden van het openbaar ministerie in het voorafgaande onderzoek, om te oordelen of aan deze vereisten is voldaan.

III. Omvang van de herziening

6. In het ontworpen artikel 39*bis* van het Wetboek van Strafvordering (artikel 2 van het ontwerp) wordt zowel gewag gemaakt van de procureur des Konings als van de arbeidsauditeur, terwijl dit niet langer het geval is in de daaropvolgende ontworpen (of een aantal, reeds bestaande) artikelen van het Wetboek van Strafvordering, waarin enkel gewag wordt gemaakt van de procureur des Konings. Het is de Raad van State niet meteen duidelijk waarop dit verschil is gebaseerd. Hierover om uitleg gevraagd, verklaarde de gemachtigde wat volgt:

"Deze discrepantie bestaat reeds in de huidige wetgeving.

Het woord "arbeidsauditeur" werd in artikel 39*bis* en in artikel 88*quater* ingevoegd door de wet van 6 juni 2010 tot invoering van het Sociaal Strafwetboek. De memorie van toelichting bij deze wet verduidelijkt dat hierdoor "de arbeidsauditeur dezelfde bevoegdheden heeft als de procureur des Konings. De sociaal inspecteurs kunnen in de hoedanigheid van officier van gerechtelijke politie het openbaar ministerie bijstaan bij een strafrechtelijk onderzoek ter bestrijding van informaticacriminaliteit" (*Parl. St.* Kamer 2008-2009, 52-1666/001, p. 324).

De misdrijven van sociaal strafrecht worden hoofdzakelijk vastgesteld door de sociaal inspecteurs. Deze oefenen hun opdracht van toezicht uit door zich te beroepen

Constitution [19]. Le projet transfère en la matière d'importantes compétences du juge d'instruction au ministère public. Même s'il ne semble pas requis que pareille ingérence soit toujours ordonnée par un juge [20] dans le cadre de l'information, il n'en reste pas moins que cet élément occupe une place importance dans le contrôle de la proportionnalité que la Cour européenne des droits de l'Homme [21] et la Cour constitutionnelle [22] effectuent en l'espèce. À cet égard, on gardera à l'esprit que le juge d'instruction est un magistrat indépendant qui mène une instruction objective, tant à charge qu'à décharge, alors que le ministère public est partie au procès pénal [23]. Il appartient au législateur, sous le contrôle toutefois des juridictions compétentes, en mettant en balance tous les intérêts en cause [24] et en tenant compte d'extensions antérieures des compétences du ministère public dans l'enquête préalable, d'apprécier si ces exigences sont remplies.

III. Ampleur de la révision

6. L'article 39*bis* en projet du Code d'instruction criminelle (article 2 du projet) mentionne tant le procureur du Roi que l'auditeur du travail, alors que tel n'est plus le cas dans les articles subséquents en projet (ou dans un certain nombre d'articles, déjà existants) du Code d'instruction criminelle, qui ne font état que du procureur du Roi. Le Conseil d'État n'aperçoit pas d'emblée sur quoi se fonde cette différence. Invité à fournir des explications à cet égard, le délégué a déclaré ce qui suit:

"Deze discrepantie bestaat reeds in de huidige wetgeving.

Het woord "arbeidsauditeur" werd in artikel 39bis en in artikel 88quater ingevoegd door de wet van 6 juni 2010 tot invoering van het Sociaal Strafwetboek. De memorie van toelichting bij deze wet verduidelijkt dat hierdoor "de arbeidsauditeur dezelfde bevoegdheden heeft als de procureur des Konings. De sociaal inspecteurs kunnen in de hoedanigheid van officier van gerechtelijke politie het openbaar ministerie bijstaan bij een strafrechtelijk onderzoek ter bestrijding van informaticacriminaliteit" (Parl. St. Kamer 2008-2009, 52-1666/001, p. 324).

De misdrijven van sociaal strafrecht worden hoofdzakelijk vastgesteld door de sociaal inspecteurs. Deze oefenen hun opdracht van toezicht uit door zich te beroepen

---

19 Zie bijvoorbeeld: EHRM 30 september 2014, *Prezhdarovi t. Bulgarije*; EHRM 4 december 2015, *Zakharov t. Rusland*; EHRM 12 januari 2016, *Szabo en Vissy t. Hongarije*.

20 C. Conings, "Het uitlezen van een gsm of ander privaat IT-systeem: This is not America", noot bij Cass. 11 februari 2015, *RW* 2015-2016, (622), 626, met verwijzingen.

21 Zie de verwijzingen aangehaald door C. Conings, *l.c.*, 626.

22 Zie bijv., specifiek inzake bijzondere opsporingsmethodes GwH 21 december 2004, nr. 202/2004, B.5.7.4 tot B.5.7.7 en B.13.2 t ot B.13.10.

23 Zie hierover ook adv.RvS 32 673/2 van 19 december 2001 over een voorontwerp dat geleid heeft tot de wet van 6 januari 2003 "betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden", *Parl.St.* Kamer, nr. 50-1688/001, (128), 140-142.

24 Zie ook GwH 19 juli 2007, nr. 105/2007, B.3.1.

19 Voir par exemple: CEDH, 30 septembre 2014, *Prezhdarovi c. Bulgarie;* CEDH, 4 décembre 2015, *Zakharov c. Russie;* CEDH, 12 janvier 2016*, Szabo et Vissy c. Hongrie*.

20 C. Conings, "Het uitlezen van een gsm of ander privaat IT-systeem: This is not America", note sous Cass., 11 février 2015, *RW* 2015-2016, (622), 626, avec références.

21 Voir les références citées par C. Conings, *l.c.,* 626.

22 Voir par exemple, spécifiquement en ce qui concerne les méthodes particulières de recherche, C.C., 21 décembre 2004, n° 202/2004, B.5.7.4 à B.5.7.7 et B.13.2 à B.13.10.

23 Voir également à ce sujet l'avis C.E. 32 673/2 du 19 décembre 2001 sur un avant-projet devenu la loi du 6 janvier 2003 "concernant les méthodes particulières de recherche et quelques autres méthodes d'enquête", *Doc. parl.,* Chambre, n° 50-1688/001, (128), pp.140-142.

24 Voir également C.C., 19 juillet 2007, n° 105/2007, B.3.1.

op hun bevoegdheden die vastgelegd zijn in het Sociaal Strafwetboek. De memorie van toelichting bij het Sociaal Strafwetboek geeft duidelijk aan dat "([d]e sociaal inspecteurs beschikken over al de bevoegdheden hen toegekend bij het Sociaal Strafwetboek" en dit zowel in de administratieve fase van de controle (vóór het opstellen van een proces-verbaal tot vaststelling van een inbreuk) als in de strafrechtelijke fase (*Parl.St.* Kamer 2008-2009, 52-1666/001, p. 106).

Het Sociaal Strafwetboek heeft de Koning de mogelijkheid gelaten om aan bepaalde sociaal inspecteurs de hoedanigheid van officier van gerechtelijke politie toe te kennen (artikelen 50 tot 52 van het Sociaal Strafwetboek). De redenering luidt als volgt:

"Deze wetsbepaling stelt de daartoe aangewezen sociaal inspecteurs in staat om bepaalde handelingen van gerechtelijke politie te verrichten die zijn voorgeschreven door het Wetboek van strafvordering, meer bepaald ter bestrijding van informaticacriminaliteit, onder het toezicht van een magistraat. Thans vervullen vele werkgevers via elektronische weg de verplichtingen die hen zijn opgelegd door de sociale wetten. Zo gebeurt bijvoorbeeld de aangifte van de arbeidsprestaties en het werknemersloon via elektronische weg. Steeds meer gegevens voorgeschreven door de sociale wetten, worden opgeslagen, verwerkt en overgedragen via een informaticasysteem. De sociaal inspecteurs moeten aldus in staat gesteld worden om kennis te nemen van dergelijke computergegevens en toezicht op de sociale wetten uit te oefenen in de context van de informaticatechnologie" (*Parl. St.* Kamer 2008-2009, 52-1666/001, p. 143).

Voor de opstellers van het Sociaal Strafwetboek was het belangrijk om aan de sociaal inspecteurs die met de hoedanigheid van officier van gerechtelijke politie zijn bekleed, de mogelijkheid te geven op te treden op grond van de bepalingen van het Wetboek van Strafvordering wanneer het dossier zich in de strafrechtelijke fase bevindt en op die manier hun technische expertise ter beschikking te stellen van het openbaar ministerie en van de onderzoeksrechter (*Parl. St*. Kamer 2008-2009, 52-1666/001, p. 143-144).

Dit is dan ook de reden waarom enkel de artikelen van het Wetboek van Strafvordering inzake informaticarecherche aangepast zijn om ook de arbeidsauditeur te vermelden."

Ook deze toelichting maakt niet duidelijk waarop dit verschil is gesteund. De stellers van het ontwerp dienen derhalve te bekijken of de onderscheiden artikelen van het Wetboek van Strafvordering inzake opsporingsonderzoek al dan niet aan een globale aanpassing toe zijn.[25]

op hun bevoegdheden die vastgelegd zijn in het Sociaal Strafwetboek. De memorie van toelichting bij het Sociaal Strafwetboek geeft duidelijk aan dat "([d]e sociaal inspecteurs beschikken over al de bevoegdheden hen toegekend bij het Sociaal Strafwetboek" en dit zowel in de administratieve fase van de controle (vóór het opstellen van een proces-verbaal tot vaststelling van een inbreuk) als in de strafrechtelijke fase (Parl. St. Kamer 2008-2009, 52-1666/001, p. 106).

Het Sociaal Strafwetboek heeft de Koning de mogelijkheid gelaten om aan bepaalde sociaal inspecteurs de hoedanigheid van officier van gerechtelijke politie toe te kennen (artikelen 50 tot 52 van het Sociaal Strafwetboek). De redenering luidt als volgt:

"Deze wetsbepaling stelt de daartoe aangewezen sociaal inspecteurs in staat om bepaalde handelingen van gerechtelijke politie te verrichten die zijn voorgeschreven door het Wetboek van strafvordering, meer bepaald ter bestrijding van informaticacriminaliteit, onder het toezicht van een magistraat. Thans vervullen vele werkgevers via elektronische weg de verplichtingen die hen zijn opgelegd door de sociale wetten. Zo gebeurt bijvoorbeeld de aangifte van de arbeidsprestaties en het werknemersloon via elektronische weg. Steeds meer gegevens voorgeschreven door de sociale wetten, worden opgeslagen, verwerkt en overgedragen via een informaticasysteem. De sociaal inspecteurs moeten aldus in staat gesteld worden om kennis te nemen van dergelijke computergegevens en toezicht op de sociale wetten uit te oefenen in de context van de informaticatechnologie" (Parl. St. Kamer 2008-2009, 52-1666/001, p. 143).

Voor de opstellers van het Sociaal Strafwetboek was het belangrijk om aan de sociaal inspecteurs die met de hoedanigheid van officier van gerechtelijke politie zijn bekleed, de mogelijkheid te geven op te treden op grond van de bepalingen van het Wetboek van Strafvordering wanneer het dossier zich in de strafrechtelijke fase bevindt en op die manier hun technische expertise ter beschikking te stellen van het openbaar ministerie en van de onderzoeksrechter (Parl. St. Kamer 2008-2009, 52-1666/001, p. 143-144).

Dit is dan ook de reden waarom enkel de artikelen van het Wetboek van Strafvordering inzake informaticarecherche aangepast zijn om ook de arbeidsauditeur te vermelden".

Ces précisions n'indiquent pas non plus clairement sur quoi cette différence est fondée. Les auteurs du projet devront dès lors examiner si les différents articles du Code d'instruction criminelle en matière d'information nécessitent ou non une adaptation globale [25].

[25] In de memorie van toelichting bij het voorontwerp van wet "tot hervorming van de rechtspleging voor de rechtbank van koophandel, tot wijziging van de rechtspositie van de gedetineerden en houdende diverse bepalingen inzake justitie", waarover de Raad van State eveneens om advies is gevraagd (zaak met rolnummer 59 226/2/3), wordt verwezen naar artikel 22 van het Wetboek van Strafvordering om te besluiten dat de arbeidsauditeur over dezelfde bevoegdheden beschikt als de procureur des Konings wat betreft de misdrijven ten aanzien waarvan hij bevoegd is. Al zou dit impliciet uit dit artikel kunnen worden afgeleid, blijft de vaststelling dat het artikel daaromtrent niet erg expliciet is.

[25] L'exposé des motifs de l'avant-projet de loi "portant réforme de la procédure devant le tribunal de commerce, modifiant le statut juridique des détenus et portant des dispositions diverses en matière de justice", sur lequel l'avis du Conseil d'État a également été demandé (inscrit au rôle sous le numéro 59 226/1/2/3) fait référence à l'article 22 du Code d'instruction criminelle pour conclure que l'auditeur du travail dispose des mêmes pouvoirs que le procureur du Roi en ce qui concerne les infractions relevant de sa compétence. Même si cette conclusion pouvait implicitement se déduire de cet article, il n'en demeure pas moins que l'article n'est pas très explicite à ce sujet.

ONDERZOEK VAN DE TEKST

Artikel 2

7. In zoverre in de in artikel 2 van het ontwerp opgenomen ontworpen bepalingen reeds bestaande regels zijn opgenomen, kan worden verwezen naar advies 28 029/2,[26] waarin met betrekking tot het legaliteitsbeginsel inzake strafrecht en strafvordering het volgende werd opgemerkt:

"c) (...)

In de ontworpen paragraaf 2 wordt de procureur des Konings ertoe gemachtigd "de aangepaste middelen aan (te wenden) om de toegang tot (in beslag genomen) gegevens ... te verhinderen". In de ontworpen tekst wordt echter niet gepreciseerd wat onder "aangepaste middelen" moet worden verstaan.

(...)

In de bespreking van deze bepaling in de memorie van toelichting is echter sprake van "techniques de cryptage" en "versleutelingstechnieken", terwijl in de voormelde Aanbeveling nr. R(95)13 gebruik wordt gemaakt van de term "chiffrement" (vercijfering).

Aangezien het in casu gaat om een regeling die verband houdt met de strafrechtelijke procedure, zouden die "aanpaste (of passende) middelen" duidelijker gedefinieerd moeten worden.

(...)

Paragraaf 4 (die de ontworpen paragraaf 5 wordt) bepaalt dat de procureur des Konings verplicht is "de verantwoordelijke van het informaticasysteem" in te lichten.

Die bepaling geeft echter niet aan wat onder "de verantwoordelijke van het informaticasysteem" moet worden verstaan.

In de zin van de voormelde Aanbeveling nr. R(95)13 geldt het begrip "persoon die voor een computersysteem verantwoordelijk is" voor alle personen die bij een opsporingsactie of een inbeslagneming formeel of werkelijk controle blijken uit te oefenen op het computersysteem waarop de opsporing betrekking heeft. Het kan gaan om de eigenaar van het systeem, om een operateur van dat systeem of zelfs om de bewaker (huurder of bewoner) van de lokalen waarin het computersysteem zich bevindt[27].

In de ontworpen bepaling dient bijgevolg uitdrukkelijk te worden bepaald welke personen moeten worden ingelicht.

Overigens kan de inbeslagneming van gegevens ook van belang zijn voor derden. Zo worden de Lid-Staten in de

[26] Adv.Rvs 28 029/2 van 31 mei 1999 over een voorontwerp dat geleid heeft tot de wet van 28 november 2000 "inzake informaticacriminaliteit", *Parl.St.*Kamer, nrs. 50-0213/001 en 50-0214/001, *54-55*.

[27] *Voetnoot 1 op blz. 52 van het geciteerde advies*: Zie blz. 34 van het rapport bij Aanbeveling nr. R (95).

EXAMEN DU TEXTE

Article 2

7. Dans la mesure où des règles préexistantes figurent dans les dispositions en projet insérées à l'article 2 du projet, il peut être renvoyé à l'avis 28 029/2 [26], dans lequel les observations suivantes ont été formulées à propos du principe de légalité en matière de droit pénal et de procédure pénale:

"c) (...)

Au paragraphe 2 en projet, le procureur du Roi est habilité à prendre "les moyens appropriés pour empêcher l'accès" aux données qui sont saisies. Le texte en projet ne précise cependant pas ce qu'il faut entendre par "moyens appropriés".

(...)

Le commentaire de cette disposition fait par contre référence à la technique du cryptage, la recommandation n° R(95)13, précitée, parle quant à elle du chiffrement.

S'agissant d'un texte touchant à la procédure pénale, il conviendrait d'identifier plus clairement ces "moyens appropriés".

(...)

Le paragraphe 4 (devenant le paragraphe 5 en projet) contient une obligation d'information à charge du procureur du Roi et destinée au "responsable du système informatique".

Mais la disposition ne donne pas une définition de ce qu'il faut entendre par "le responsable du système informatique".

Au sens de la recommandation n° R(95)13, précitée, la notion englobe toutes les personnes qui, lors de la perquisition ou de la saisie, paraissent disposer formellement ou réellement du contrôle sur le système informatique, objet de la perquisition. Il peut s'agir du propriétaire du système, d'un opérateur de ce système ou même du gardien (locataire ou occupant) des locaux abritant le système informatique [27].

La disposition en projet doit, en conséquence, définir expressément les personnes concernées par l'information.

Par ailleurs, la saisie de données peut également concerner des tierces personnes. C'est ainsi que la recommandation

[26] Avis C.E. 28 029/2 du 31 mai 1999 sur un avant-projet devenu la loi du 28 novembre 2000 "relative à la criminalité informatique", *Doc. parl.,* Chambre, nos 50-0213/001 et 50-0214/001, pp. 54-55.

[27] *Note 1 à la page 24 de l'avis cité:* Voir p. 34 du rapport accompagnant la recommandation n° R(95)13.

voormelde Aanbeveling nr. R(95)13 verzocht dit verstrekken van inlichtingen te regelen met oog voor de noden van het onderzoek[28].

Dat vereiste is van belang, aangezien eenieder die zich door een opsporingshandeling of een onderzoekshandeling met betrekking tot zijn goederen geschaad acht, krachtens de artikelen 28*sexies* en 61*quater* van het Wetboek van Strafvordering aan de procureur des Konings of aan de onderzoeksrechter de opheffing ervan kan vragen.

In dat verband biedt de ontworpen paragraaf 2, tweede lid, nauwelijks duidelijkheid doordat daarin wordt bepaald dat de procureur des Konings "evenwel het verdere gebruik van het geheel of een deel van deze gegevens (kan) toestaan, wanneer dit geen gevaar voor de strafvordering oplevert."."

Bovendien rijst de vraag of het ook geen aanbeveling verdient andere begrippen nader te definiëren, zoals "informaticasysteem"[29], "exploitatie"[30] en "valse sleutels". Op zijn minst dienen zulke begrippen in de memorie van toelichting te worden verduidelijkt, het best aan de hand van concrete voorbeelden.

8. Het is de Raad van State niet duidelijk waarom in het ontworpen artikel 39*bis*, § 2, eerste lid, van het Wetboek van Strafvordering (artikel 2, 2°, van het ontwerp) gewag wordt gemaakt van het "wettelijk" in beslag zijn genomen.[31] Het is evident dat elke inbeslagname conform de wet dient te gebeuren, doch dat hoeft niet uitdrukkelijk te worden bepaald.

9. Over het ontworpen artikel 39*bis,* § 2, tweede lid, van het Wetboek van Strafvordering verschafte de gemachtigde de volgende toelichting:

"De woorden "Onverminderd de exploitatie die voortvloeit uit de inbeslagname" in § 2, tweede lid hebben enkel tot doel de verhouding te verduidelijken tussen het eerste en het tweede lid van deze paragraaf. Het eerste lid betreft de informaticasystemen die in beslag genomen zijn. Het tweede lid betreft de systemen die in beslag genomen kunnen worden. De aanhef van het tweede lid beoogt elke onzekerheid te vermijden en te verduidelijken dat het tweede lid niet mag begrepen worden alsof het de strekking van het eerste lid zou

[28] Voetnoot 2 op blz. 52 van het geciteerde advies: Zie blz. 35 van het rapport.

[29] De gemachtigde verklaarde hierover het volgende: "De term "informaticasysteem" wordt reeds gehanteerd in de huidige versie van het Wetboek van Strafvordering. Het werd geïntroduceerd door de wet van 28 november 2000 inzake informaticacriminaliteit. In de memorie van toelichting bij die wet wordt het begrip als volgt omschreven: "Hiermee wordt gedoeld op alle systemen voor de opslag, verwerking of overdracht van data. Hierbij wordt vooral gedacht aan computers, chipkaarten en dergelijke, maar ook aan netwerken en delen daarvan, evenals aan telecommunicatiesystemen of onderdelen daarvan die een beroep doen op IT" (*Parl.St.* Kamer 1992-2000, 50-213/001, p. 12)."

[30] Volgens de gemachtigde gaat het om het uitlezen van de gegevens die op een informaticasysteem te vinden zijn. Dit zou het best in de tekst zelf worden geëxpliciteerd zo het woord "exploitatie" erin behouden blijft (zie opmerking 9 *in fine*).

[31] De gemachtigde verklaarde dat hierdoor impliciet wordt verwezen naar de regels voor inbeslagname die onder meer vervat liggen in artikel 35 van het Wetboek van Strafvordering.

n° R(95)13, précitée, invite les États membres à organiser ce type d'information et ce dans le respect des impératifs de l'enquête [28].

Cette exigence est importante car, en vertu des articles 28*sexies* et 61*quater* du Code d'instruction criminelle, toute personne qui s'estime lésée par un acte d'information ou par un acte d'instruction relatif à ses biens peut en demander la levée soit au procureur du Roi, soit au juge d'instruction.

À cet égard, le paragraphe 2, alinéa 2, en projet, n'est guère explicite lorsqu'il dispose que le procureur du Roi "peut cependant autoriser l'usage ultérieur de l'ensemble ou d'une partie de ces données, lorsque cela ne présente pas de danger pour l'exercice des poursuites."".

En outre, la question se pose de savoir s'il n'est pas également recommandé de définir de façon plus précise d'autres notions, telles que "système informatique" [29], "exploitation" [30] et "fausses clés". Pareilles notions doivent à tout le moins être précisées dans l'exposé des motifs, de préférence sur la base d'exemples concrets.

8. Le Conseil d'État n'aperçoit pas pourquoi l'article 39*bis*, § 2, alinéa 1er, en projet, du Code d'instruction criminelle (article 2, 2°, du projet) fait état d'un système "légalement" saisi [31]. Il est évident que toute saisie doit intervenir en conformité avec la loi, sans qu'il soit nécessaire de le préciser expressément.

9. À propos de l'article 39*bis*, § 2, alinéa 2, en projet, du Code d'instruction criminelle, le délégué a donné les précisions suivantes:

"De woorden "Onverminderd de exploitatie die voortvloeit uit de inbeslagname" in § 2, tweede lid hebben enkel tot doel de verhouding te verduidelijken tussen het eerste en het tweede lid van deze paragraaf. Het eerste lid betreft de informaticasystemen die in beslag genomen zijn. Het tweede lid betreft de systemen die in beslag genomen kunnen worden. De aanhef van het tweede lid beoogt elke onzekerheid te vermijden en te verduidelijken dat het tweede lid niet mag begrepen worden alsof het de strekking van het eerste lid zou

[28] Note 2 à la page 24 de l'avis cité: Voir p. 35 du rapport.

[29] À ce sujet, le délégué a déclaré ce qui suit: "De term "informaticasysteem" wordt reeds gehanteerd in de huidige versie van het Wetboek van Strafvordering. Het werd geïntroduceerd door de wet van 28 november 2000 inzake informaticacriminaliteit. In de memorie van toelichting bij die wet wordt het begrip als volgt omschreven: "Hiermee wordt gedoeld op alle systemen voor de opslag, verwerking of overdracht van data. Hierbij wordt vooral gedacht aan computers, chipkaarten en dergelijke, maar ook aan netwerken en delen daarvan, evenals aan telecommunicatiesystemen of onderdelen daarvan die een beroep doen op IT" (*Parl.St.* Kamer 1992-2000, 50-213/001, p. 12)".

[30] Selon le délégué, il s'agit de la lecture de données que l'on trouve dans un système informatique. Mieux vaudrait le préciser dans le texte même dans l'hypothèse où le mot "exploitation" y est maintenu (voir l'observation 9 *in fine*).

[31] Le délégué a déclaré qu'il est ainsi fait implicitement référence aux règles en matière de saisie qui figurent notamment à l'article 35 du Code d'instruction criminelle.

beperken. Indien het informaticasysteem in beslag genomen is, kan de officier van gerechtelijke politie beslissen tot de exploitatie van de gegevens van dit systeem, zonder dat een beslissing van de procureur des Konings of arbeidsauditeur vereist is."

De aldus toegelichte draagwijdte van die bepaling zou in ieder geval b*eter* in de tekst ervan tot uiting moeten komen, waarbij de vraag rijst of het inleidende zinsdeel van de genoemde bepaling gehandhaafd dient te blijven.

10. Overeenkomstig hetzelfde ontworpen artikel 39*bis*, § 2, tweede lid, van het Wetboek van Strafvordering kan de procureur des Konings of de arbeidsauditeur een zoeking bevelen in een informaticasysteem of in een deel ervan dat door hem in beslag kan worden genomen. In de memorie van toelichting wordt vooropgesteld dat elke externe verbinding door de politiediensten dient te worden uitgeschakeld. Gevraagd of dit niet moet worden opgenomen in de tekst zelf van het ontwerp, antwoordde de gemachtigde wat volgt:

"Ons inziens is het niet noodzakelijk om dit in de wet zelf op te nemen. Uit de samenlezing van § 2 met § 4 (die handelt over de uitbreiding van de zoeking "naar een informaticasysteem of een deel daarvan dat zich op een andere plaats bevindt"), blijkt reeds duidelijk *a contrario* dat de toepassing van § 2 beperkt is tot het informaticasysteem zelf waarin de zoeking wordt uitgevoerd. De enige manier om er zeker van te zijn dat enkel het informaticasysteem op zich geëxploiteerd wordt, lijkt ons te zijn dat gewerkt wordt in een Faraday-omgeving. De memorie geeft op dit vlak dus slechts verduidelijking bij de tekst van het gewijzigde artikel 39*bis*."

Omwille van de rechtszekerheid lijkt het toch raadzaam om dit te expliciteren in de tekst zelf van het ontwerp.

11. De in het ontworpen artikel 39*bis,* § 3, eerste lid, van het Wetboek van Strafvordering (artikel 2, 3°, van het ontwerp) bedoelde gegevens kunnen in geval van dringendheid of omwille van technische redenen worden gekopieerd op dragers die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken. Vraag is of er in dit geval niet moet worden voorzien in een vergoedingsregeling.

12. Om uitleg gevraagd omtrent het ontworpen artikel 39*bis,* § 3, derde lid, van het Wetboek van Strafvordering, waarvan de Nederlandse en de Franse tekst discordant zijn, verklaarde de gemachtigde wat volgt:

"Het betreft een vergetelheid. In de Nederlandse tekst moet het woord "hij" vervangen worden door de woorden "de procureur des Konings of de arbeidsauditeur". In de Franse tekst moet staan "*le procureur du Roi ou l'auditeur du travail*"."

De genoemde bepaling dient in die zin te worden aangepast.

13. In de memorie van toelichting wordt verduidelijkt dat het ontworpen artikel 39*bis*, § 4, van het Wetboek van Strafvordering (artikel 2, 4°, van het ontwerp) enkel betrekking heeft op niet-heimelijke zoekingen. Gevraagd waaruit dit in de tekst van die bepaling blijkt, antwoordde de gemachtigde:

beperken. Indien het informaticasysteem in beslag genomen is, kan de officier van gerechtelijke politie beslissen tot de exploitatie van de gegevens van dit systeem, zonder dat een beslissing van de procureur des Konings of arbeidsauditeur vereist is".

La portée ainsi précisée de cette disposition devrait en tout cas apparaître dans le texte de celle-ci, la question se posant alors de savoir si le membre de phrase introductif de la disposition citée doit être maintenu.

10. Conformément au même article 39*bis*, § 2, alinéa 2, en projet, du Code d'instruction criminelle, le procureur du Roi ou l'auditeur de travail peut ordonner une recherche dans un système informatique ou une partie de celui-ci qui peut être saisi par lui. L'exposé des motifs indique que chaque liaison externe doit être désactivée par les services de police. Interrogé sur la question de savoir s'il ne faut pas insérer cette précision dans le texte même du projet, le délégué a répondu ce qui suit:

"*Ons inziens is het niet noodzakelijk om dit in de wet zelf op te nemen. Uit de samenlezing van § 2 met § 4 (die handelt over de uitbreiding van de zoeking "naar een informaticasysteem of een deel daarvan dat zich op een andere plaats bevindt"), blijkt reeds duidelijk a contrario dat de toepassing van § 2 beperkt is tot het informaticasysteem zelf waarin de zoeking wordt uitgevoerd. De enige manier om er zeker van te zijn dat enkel het informaticasysteem op zich geëxploiteerd wordt, lijkt ons te zijn dat gewerkt wordt in een Faraday-omgeving. De memorie geeft op dit vlak dus slechts verduidelijking bij de tekst van het gewijzigde artikel 39bis*".

Dans un souci de sécurité juridique, il paraît néanmoins indiqué de préciser ce point dans le texte même du projet.

11. En cas d'urgence ou pour des raisons techniques, les données visées à l'article 39*bis*, § 3, alinéa 1er, en projet, du Code d'instruction criminelle (article 2, 3°, du projet) peuvent être copiées sur des supports qui sont à la disposition des personnes autorisées à utiliser le système informatique. La question se pose de savoir s'il ne faut pas prévoir, dans ce cas, un régime d'indemnisation.

12. Invité à donner des éclaircissements à propos de l'article 39*bis*, § 3, alinéa 3, en projet, du Code d'instruction criminelle, dont les textes français et néerlandais présentent des discordances, le délégué a déclaré ce qui suit:

"*Het betreft een vergetelheid. In de Nederlandse tekst moet het woord "hij" vervangen worden door de woorden "de procureur des Konings of de arbeidsauditeur". In de Franse tekst moet staan* "le procureur du Roi ou l'auditeur du travail"".

Il convient d'adapter la disposition citée en ce sens.

13. L'exposé des motifs précise que l'article 39*bis*, § 4, en projet, du Code d'instruction criminelle (article 2, 4°, du projet) ne concerne que des recherches non secrètes. À la question de savoir où se trouve cet élément dans le texte de la disposition, le délégué a répondu ce qui suit:

"De niet-heimelijkheid van alle zoekingen die in artikel 39*bis* zijn opgenomen, vloeit voort uit artikel 39*bis*, § 5. Deze paragraaf voorziet in de principiële verplichting om de verantwoordelijke van het informaticasysteem op de hoogte te brengen van de zoeking in het informaticasysteem of de uitbreiding ervan, tenzij diens identiteit of woonplaats redelijkerwijze niet achterhaald kan worden. Ook moet deze verantwoordelijke in voorkomend geval een samenvatting meegedeeld worden van de gegevens die zijn gekopieerd, ontoegankelijk gemaakt of verwijderd.

Bovendien blijkt het niet-heimelijke karakter *a contrario* uit de samenlezing met het nieuwe artikel 90*ter* Sv., dat voor de zoeking vervat in dat artikel wél expliciet een heimelijk oogmerk vermeldt (§ 1), en dat bepaalt dat de maatregel van artikel 90*ter* bestaat "onverminderd de toepassing van [artikel] 39*bis*"."

Het blijft evenwel de vraag of het niet-heimelijke karakter van de zoeking niet be*ter* in de tekst van het ontworpen artikel 39*bis*, § 4, van het Wetboek van Strafvordering tot uiting zou dienen te komen. In dat artikel wordt overigens niet uitgesloten dat de verantwoordelijke van het informaticasysteem niet van de zoeking op de hoogte zal zijn omdat men ofwel zijn identiteit, ofwel zijn woonplaats niet kent. Uit de tekst van het ontworpen artikel 39*bis*, § 5, van het Wetboek van Strafvordering (artikel 2, 7°, van het ontwerp) blijkt overigens niet dat men vooraf op de hoogte moet worden gesteld van de zoeking.

14. Volgens de in de memorie van toelichting opgenomen uitleg bij het ontworpen artikel 39*bis*, § 4, van het Wetboek van Strafvordering is de daarin aan de procureur des Konings of de arbeidsauditeur toegekende bevoegdheid beperkt aangezien hij geen gebruik mag maken van nieuwe "valse sleutels" om de zoeking uit te breiden tot informaticanetwerken die zich op een andere plaats bevinden dan waar de zoeking plaatsvindt. De gemachtigde voegde daar nog het volgende aan toe:

"Het begrip "nieuwe valse sleutels" staat niet in de tekst van het voorontwerp zelf. Het wordt gebruikt in de memorie van toelichting om het verschil aan te duiden met de valse sleutels (bv. een wachtwoord) die vereist waren om toegang te krijgen tot het informaticasysteem zelf. Elk additionele gebruik van valse sleutels dat vereist is teneinde de uitbreiding van de zoeking (conform § 4 van artikel 39*bis*) te kunnen uitvoeren, vereist een machtiging van de onderzoeksrechter. Dit is eveneens het geval indien het paswoord, nodig voor de uitbreiding van de zoeking (§ 4), hetzelfde zou blijken te zijn als het paswoord dat nodig was om toegang te krijgen tot het informaticasysteem zelf (§ 2).

Om het met andere woorden te stellen: voor de uitbreiding van een zoeking zal het verplicht zijn zich te wenden tot de onderzoeksrechter wanneer een nieuwe poging tot decodering of "hacking" nodig is bovenop deze die nodig was om binnen te dringen in het informaticasysteem.

Voorbeeld: zo is er geen nieuwe poging tot decryptie of "hacking" vereist om toegang te verkrijgen tot de Facebookaccount via de Facebook-app op de smartphone die inbeslaggenomen is en waartoe de speurders toegang hebben

"De niet-heimelijkheid van alle zoekingen die in artikel 39bis zijn opgenomen, vloeit voort uit artikel 39bis, § 5. Deze paragraaf voorziet in de principiële verplichting om de verantwoordelijke van het informaticasysteem op de hoogte te brengen van de zoeking in het informaticasysteem of de uitbreiding ervan, tenzij diens identiteit of woonplaats redelijkerwijze niet achterhaald kan worden. Ook moet deze verantwoordelijke in voorkomend geval een samenvatting meegedeeld worden van de gegevens die zijn gekopieerd, ontoegankelijk gemaakt of verwijderd.

Bovendien blijkt het niet-heimelijke karakter a contrario uit de samenlezing met het nieuwe artikel 90ter Sv., dat voor de zoeking vervat in dat artikel wél expliciet een heimelijk oogmerk vermeldt (§ 1), en dat bepaalt dat de maatregel van artikel 90ter bestaat "onverminderd de toepassing van [artikel] 39bis"".

La question demeure toutefois de savoir s'il ne vaudrait pas mieux faire apparaître le caractère non secret de la recherche dans le texte de l'article 39*bis*, § 4, en projet, du Code d'instruction criminelle. Cet article n'exclut d'ailleurs pas que le responsable du système informatique ne sera pas informé de la recherche, parce que son identité ou son domicile est inconnu. Au demeurant, il ne résulte pas du texte de l'article 39*bis*, § 5, en projet, du Code d'instruction criminelle (article 2, 7°, du projet) qu'il faut être préalablement informé de la recherche.

14. Selon le commentaire figurant dans l'exposé des motifs à propos de l'article 39*bis*, § 4, en projet, du Code d'instruction criminelle, le pouvoir qu'il attribue au procureur du Roi ou à l'auditeur du travail est limité étant donné qu'il ne peut pas faire usage de nouvelles "fausses clés" pour étendre la recherche vers des réseaux informatiques qui se trouvent dans un autre lieu que celui où la recherche est effectuée. Le délégué a encore ajouté ce qui suit:

"Het begrip 'nieuwe valse sleutels" staat niet in de tekst van het voorontwerp zelf. Het wordt gebruikt in de memorie van toelichting om het verschil aan te duiden met de valse sleutels (bv. een wachtwoord) die vereist waren om toegang te krijgen tot het informaticasysteem zelf. Elk additionele gebruik van valse sleutels dat vereist is teneinde de uitbreiding van de zoeking (conform § 4 van artikel 39bis) te kunnen uitvoeren, vereist een machtiging van de onderzoeksrechter. Dit is eveneens het geval indien het paswoord, nodig voor de uitbreiding van de zoeking (§ 4), hetzelfde zou blijken te zijn als het paswoord dat nodig was om toegang te krijgen tot het informaticasysteem zelf (§ 2).

Om het met andere woorden te stellen: voor de uitbreiding van een zoeking zal het verplicht zijn zich te wenden tot de onderzoeksrechter wanneer een nieuwe poging tot decodering of "hacking" nodig is bovenop deze die nodig was om binnen te dringen in het informaticasysteem.

Voorbeeld: zo is er geen nieuwe poging tot decryptie of "hacking" vereist om toegang te verkrijgen tot de Facebookaccount via de Facebook-app op de smartphone die inbeslaggenomen is en waartoe de speurders toegang hebben

kunnen verkrijgen (hetzij omdat deze smartphone niet beveiligd was, hetzij omdat ze erin geslaagd zijn, met machtiging van de procureur des Konings, het toestel te "hacken" en er zo in binnen te dringen). De procureur des Konings kan dus de kennisname bevelen van de Facebookgegevens die zich reeds op de smartphone bevinden op het moment van de inbeslagname, maar hij kan ook het bijwerken (updaten) van de Facebookgegevens bevelen en dus de kennisname van de gegevens die misschien nog niet fysiek op de smartphone staan op het moment van de inbeslagneming ervan. Het feit dat het wachtwoord hetzelfde of verschillend is, is niet van belang. Het doorslaggevend criterium is de (al dan niet) noodzaak om een wachtwoord in te geven op het moment dat de speurders toegang willen verkrijgen tot de gegevens van de "cloud". Indien het wachtwoord door het informaticasysteem "onthouden" werd, en dus niet meer moet ingegeven worden, moet er geen nieuwe stap genomen worden en kan de procureur de uitbreiding van de zoeking machtigen. Indien men daarentegen opnieuw een wachtwoord moet ingeven (zelfs indien het in werkelijkheid om hetzelfde wachtwoord gaat dat gebruikt werd om de toegang tot het besturingssysteem van de smartphone te beveiligen), is voor de uitbreiding naar de gegevens in de "cloud" een machtiging van de onderzoeksrechter vereist."

Vraag is evenwel of het al dan niet optreden van de onderzoeksrechter, en derhalve het bestaan van een bijkomende waarborg, mag afhangen van de loutere mogelijkheid van een informaticasysteem om, zoals de gemachtigde schetste, een wachtwoord te "onthouden".

15. Er dient in het ontworpen artikel 39*bis*, § 4, van het Wetboek van Strafvordering te worden verduidelijkt dat de uitbreiding van de zoeking betrekking heeft op de zoekingen in informaticasystemen of in een deel ervan die in beslag zijn genomen of in beslag kunnen worden genomen overeenkomstig het ontworpen artikel 39*bis*, § 2, van dat wetboek.

16. In het ontworpen artikel 39*bis*, § 4*bis*, van het Wetboek van Strafvordering (artikel 2, 5°, van het ontwerp) wordt het bevelen van een andere zoeking dan de zoekingen bedoeld in het ontworpen artikel 39*bis*, §§ 2 en 4, van dat wetboek voorbehouden aan de onderzoeksrechter. In de memorie van toelichting wordt dit als volgt verduidelijkt:

"[H]et vierde niveau betreft een restcategorie, namelijk de informaticasystemen die niet vatbaar zijn voor inbeslagneming. (…)

Voorbeeld: de onderzoekers weten, bijvoorbeeld via bijzondere opsporingsmethoden, dat de verdachte een Gmail-account heeft, maar hebben geen enkel toestel in beslag genomen dat verbonden is aan die Gmail-account, waardoor de uitbreiding van de zoeking bedoeld in paragraaf 4 niet toepasselijk is."

Hieruit lijkt voort te vloeien dat in het ontworpen artikel 39*bis*, § 4*bis*, van het Wetboek van Strafvordering wordt verwezen naar een informaticasysteem dat feitelijk niet in beslag kan worden genomen, terwijl in het ontworpen artikel 39*bis*, § 2, van dat wetboek eerder lijkt te worden verwezen naar een juridische mogelijkheid om in beslag

kunnen verkrijgen (hetzij omdat deze smartphone niet beveiligd was, hetzij omdat ze erin geslaagd zijn, met machtiging van de procureur des Konings, het toestel te "hacken" en er zo in binnen te dringen). De procureur des Konings kan dus de kennisname bevelen van de Facebookgegevens die zich reeds op de smartphone bevinden op het moment van de inbeslagname, maar hij kan ook het bijwerken (updaten) van de Facebookgegevens bevelen en dus de kennisname van de gegevens die misschien nog niet fysiek op de smartphone staan op het moment van de inbeslagneming ervan. Het feit dat het wachtwoord hetzelfde of verschillend is, is niet van belang. Het doorslaggevend criterium is de (al dan niet) noodzaak om een wachtwoord in te geven op het moment dat de speurders toegang willen verkrijgen tot de gegevens van de "cloud". Indien het wachtwoord door het informaticasysteem "onthouden" werd, en dus niet meer moet ingegeven worden, moet er geen nieuwe stap genomen worden en kan de procureur de uitbreiding van de zoeking machtigen. Indien men daarentegen opnieuw een wachtwoord moet ingeven (zelfs indien het in werkelijkheid om hetzelfde wachtwoord gaat dat gebruikt werd om de toegang tot het besturingssysteem van de smartphone te beveiligen), is voor de uitbreiding naar de gegevens in de "cloud" een machtiging van de onderzoeksrechter vereist".

La question se pose toutefois de savoir si l'intervention ou non du juge d'instruction, et partant l'existence d'une garantie supplémentaire, peut être tributaire de la simple possibilité qu'un système informatique "retienne" un mot de passe, pour reprendre les propos du délégué.

15. L'article 39*bis*, § 4, en projet, du Code d'instruction criminelle doit préciser que l'extension de la recherche concerne les recherches effectuées dans des systèmes informatiques ou une partie de ceux-ci qui sont ou peuvent être saisis conformément à l'article 39*bis*, § 2, en projet, de ce code.

16. L'article 39*bis*, § 4*bis*, en projet, du Code d'instruction criminelle (article 2, 5°, du projet) laisse au seul juge d'instruction le soin d'ordonner une recherche autre que les recherches visées à l'article 39*bis*, §§ 2 et 4, en projet, de ce code. L'exposé des motifs précise ce point comme suit:

"[L]e troisième [lire: quatrième] niveau concerne les systèmes informatiques qui ne sont pas susceptibles de saisie. (…)

Exemple: les enquêteurs savent, par exemple via des méthodes particulières de recherche, que le suspect a un compte Gmail mais n'ont saisi aucun appareil connecté à ce compte Gmail de sorte que l'extension de la recherche visée au paragraphe 4 n'est pas applicable".

Il semble en découler que l'article 39*bis*, § 4*bis*, en projet, du Code d'instruction criminelle vise un système informatique qui, en fait, ne peut pas être saisi, alors que l'article 39*bis*, § 2, en projet, de ce code paraît plutôt viser une possibilité juridique de saisie. Ce distinguo devrait apparaître plus clairement dans le texte des dispositions citées. En outre, la

te nemen. Dit zou dan b*eter* in de tekst van de genoemde bepalingen tot uiting dienen te komen. Tevens rijst de vraag of ook niet dient te worden bepaald dat de onderzoeksrechter de verantwoordelijke van het informaticasysteem op de hoogte dient te brengen van de zoeking, naar analogie van wat voor de procureur des Konings of de arbeidsauditeur is bepaald in het ontworpen artikel 39*bis*, § 5, van het Wetboek van Strafvordering.

17. Los van hetgeen is opgemerkt in opmerking 16, rijst de vraag of het onderscheid inzake de waarborgen met betrekking tot zoekingen in informaticasystemen naargelang ze al dan niet (feitelijk) in beslag kunnen worden genomen, wel pertinent is.[32] Binnen de toegemeten tijd kon deze kwestie evenwel niet nader worden onderzocht.

18. Er dient in het ontworpen artikel 39*bis*, § 5, van het Wetboek van Strafvordering, dat overigens b*eter* zou aanvangen met "Tenzij diens identiteit niet achterhaald kan worden, brengt ...", te worden bepaald wanneer de erin bedoelde mededeling dient plaats te vinden (onverwijld na het verrichten van de zoeking?).

Artikel 3

19. Luidens het ontworpen artikel 39*ter*, § 4, van het Wetboek van Strafvordering dienen de bewaarde gegevens volgens de toepasselijke wetsbepalingen te worden bezorgd (niet: "overgemaakt") aan de bevoegde gerechtelijke autoriteiten. Het heeft geen zin te bepalen dat dit bezorgen dient te gebeuren volgens "de toepasselijke wetsbepalingen" omdat die bepalingen uit zichzelf reeds van toepassing zijn. Zo het de bedoeling is gevolg te geven aan artikel 17, lid 1, b, van het Cybercrimeverdrag, op grond waarvan die mededeling vlug of zo vlug mogelijk ("rapide" – "expeditious") dient te gebeuren, moeten, zo de bestaande wetsbepalingen daartoe geen waarborg inhouden, daartoe de nodige regels worden ingevoerd.

Artikel 4

20. De in het ontworpen artikel 39*quater*, §§ 1 en 2, van het Wetboek van Strafvordering vervatte delegaties dienen aan de Koning te worden verleend in plaats van aan de minister bevoegd voor justitie (niet: "de minister van Justitie"). De wetgever vermag zich immers in beginsel niet te mengen in de organisatie van de uitvoerende macht, die overeenkomstig artikel 37 van de Grondwet bij de Koning berust. Het komt derhalve hem, en niet de wetgever, toe om delegaties aan ministers te verlenen, in acht genomen de grenzen waarbinnen subdelegaties mogelijk zijn.[33]

Een gelijkaardige opmerking geldt ten aanzien van tal van andere ontworpen bepalingen.

21. Hoewel het in het ontworpen artikel 39*quater*, § 2, vierde lid, tweede streepje (lees: 2°), van het Wetboek van

[32] Zie C. Conings, *l.c.*, 623-624.

[33] In het ontworpen artikel 46*bis*, § 1, tweede en vierde lid, van het Wetboek van Strafvordering (artikel 5 van het ontwerp) wordt de delegatie wel aan de Koning verleend.

question se pose de savoir s'il ne faut pas également prévoir que le juge d'instruction est tenu d'informer le responsable du système informatique de la recherche, par analogie avec ce que l'article 39*bis*, § 5, en projet, du Code d'instruction criminelle prévoit pour le procureur du Roi ou l'auditeur du travail.

17. Outre ce qui a été relevé dans l'observation 16, on peut se demander si la distinction opérée en matière de garanties relatives aux recherches dans les systèmes informatiques, selon qu'ils peuvent ou non être saisis (en fait), est bel et bien pertinente [32]. Cette question n'a toutefois pas pu être examinée plus en détail dans le délai imparti.

18. L'article 39*bis*, § 5, en projet, du Code d'instruction criminelle, qu'il est par ailleurs préférable de faire commencer par "Sauf si son identité ne peut être retrouvée, le procureur...", doit préciser à quel moment la communication qui y est visée doit avoir lieu (sans délai après l'accomplissement de la recherche?).

Article 3

19. Selon l'article 39*ter*, § 4, en projet, du Code d'instruction criminelle, les données conservées doivent être transmises aux autorités judiciaires compétentes selon les dispositions légales applicables. Il est inutile de prévoir que cette transmission doit être effectuée selon "les dispositions légales applicables", parce que ces dispositions s'appliquent déjà par elles-mêmes. Si l'intention est de donner suite à l'article 17, paragraphe 1, b), de la Convention sur la cybercriminalité, en vertu duquel cette communication doit s'opérer rapidement ou le plus rapidement possible, les règles nécessaires à cet effet doivent être instaurées si les dispositions légales existantes n'impliquent pas de garanties à cet égard.

Article 4

20. Les délégations inscrites à l'article 39*quater*, §§ 1er et 2, en projet, du Code d'instruction criminelle doivent être conférées au Roi plutôt qu'au ministre qui a la Justice dans ses attributions (et non au: "ministre de la Justice"). En effet, le législateur ne peut en principe s'immiscer dans l'organisation du pouvoir exécutif qui, conformément à l'article 37 de la Constitution, appartient au Roi. Il revient dès lors à ce dernier, et non au législateur, d'accorder des délégations aux ministres, en tenant compte des limites dans lesquelles des subdélégations sont possibles [33].

Une observation similaire peut être formulée à l'égard de nombreuses autres dispositions en projet.

21. Bien que la notion de "intérêts essentiels de la Belgique" utilisée à l'article 39*quater*, § 2, alinéa 4, deuxième tiret (lire:

[32] Voir C. Conings, *l.c.,* 623-624.

[33] L'article 46*bis*, § 1er, alinéas 2 et 4, en projet, du Code d'instruction criminelle (article 5 du projet) confère bel et bien cette délégation au Roi.

Strafvordering gehanteerde begrip “wezenlijke belangen van België” teruggaat op de artikelen 29, lid 5, en 30, lid 2, van het Cybercrimeverdrag, rijst toch de vraag of geen nadere invulling dient te worden gegeven aan dat op zich nogal vage begrip.

Artikel 5

22. Er dient te worden verduidelijkt wat de juiste draagwijdte is van de in het ontworpen artikel 46*bis*, § 2, eerste lid, van het Wetboek van Strafvordering (artikel 5, 2°, van het ontwerp) voorkomende woorden “termijn waarvan de modaliteiten vastgesteld worden door de Koning” nu daarvoor geen gewag wordt gemaakt van een “termijn”, maar wel van een “tijdstip bepaald in de vordering”.

Eenzelfde opmerking geldt ten aanzien van het ontworpen artikel 88*bis*, § 4, eerste lid, van het Wetboek van Strafvordering (artikel 12, 3°, van het ontwerp).

Artikel 6

23. Men schrijve in het ontworpen artikel 46*quinquies*, § 1, eerste lid, van het Wetboek van Strafvordering (artikel 6, 1°, van het ontwerp) “en gesloten voorwerpen die zich op deze plaats bevinden te openen“in plaats van “met inbegrip van het openen van gesloten voorwerpen die zich op deze plaats bevinden”, en dienvolgens in het ontworpen artikel 46*quinquies*, § 2, van dat wetboek (artikel 6, 2°, van het ontwerp) “en het openen” in plaats van “met inbegrip van het openen”.

Artikel 7

24. Het ontworpen artikel 46*sexies* van het Wetboek van Strafvordering is geïnspireerd op het bestaande artikel 47*quinquies*, §§ 2 en 3, van dat wetboek. Er kan dan ook in de eerste plaats worden verwezen naar de opmerkingen over die laatste bepalingen in advies 32 673/2, luidend:

“3. Het plegen van strafbare feiten

a) Het ontworpen artikel 47*quinquies*, § 1, van het Wetboek van Strafvordering bepaalt dat politieambtenaren, belast met de uitvoering van de bijzondere opsporingsmethoden, geen strafbare feiten mogen plegen in het kader van hun opdracht.

In de ontworpen paragraaf 2 van diezelfde bepaling wordt evenwel gestipuleerd dat zij “vrij(blijven) van straf”, wanneer zij in het kader van hun opdracht en met het oog op het welslagen ervan of ter verzekering van hun eigen veiligheid of die van andere bij de operatie betrokken personen, toch strikt noodzakelijke strafbare feiten plegen, doch met uitdrukkelijk goedvinden van de procureur des Konings.

Zoals bepaalde auteurs benadrukken is het plegen van strafbare feiten in het kader van de bijzondere opsporingsmethoden soms noodzakelijk. Er moeten evenwel twee categorieën van strafbare feiten onderscheiden worden. Hoewel de eerste categorie geen problemen oplevert, aangezien het in

2°), en projet, du Code d’instruction criminelle, se retrouve dans les articles 29, paragraphe 5, et 30, paragraphe 2, de la Convention sur la cybercriminalité, la question se pose néanmoins de savoir s’il ne faut pas préciser cette notion relativement vague en soi.

Article 5

22. Il convient de préciser la portée exacte des mots “délai dont les modalités sont fixées par le Roi” figurant à l’article 46*bis*, § 2, alinéa 1er, en projet, du Code d’instruction criminelle (article 5, 2°, du projet), puisque’il n’y est pas question d’un “délai”, mais d’un “moment précisé dans la réquisition”.

La même observation vaut pour l’article 88*bis*, § 4, alinéa 1er, en projet, du Code d’instruction criminelle (article 12, 3°, du projet).

Article 6

23. À l’article 46*quinquies*, § 1er, alinéa 1er, en projet, du Code d’instruction criminelle (article 6, 1°, du projet), on écrira “et à ouvrir les objets fermés se trouvant dans ce lieu” au lieu de “en ce compris ouvrir les objets fermés se trouvant dans ce lieu” et, partant, à l’article 46*quinquies*, § 2, en projet, de ce code (article 6, 2°, du projet), on écrira “et l’ouverture” au lieu de “en ce compris l’ouverture”.

Article 7

24. L’article 46*sexies* en projet du Code d’instruction criminelle s’inspire de l’article 47*quinquies*, §§ 2 et 3, existant de ce code. On pourra dès lors se référer en premier lieu aux observations formulées à propos de ces dernières dispositions dans l’avis 32 673/2:

“3. La perpétration d’infractions

a) L’article 47*quinquies*, § 1er, en projet, du Code d’instruction criminelle interdit aux fonctionnaires de police chargés d’exécuter une méthode particulière de recherche de commettre des infractions dans le cadre de leur mission.

Cependant, le paragraphe 2, en projet, de cette même disposition prévoit qu’ils “sont exemptés de peine” lorsque, dans le cadre de leur mission et en vue de la réussite de celle-ci ou afin de garantir leur propre sécurité ou celle d’autres personnes impliquées dans l’opération, ils commettent néanmoins des infractions absolument nécessaires, mais avec l’accord exprès du procureur du Roi.

Ainsi que le soulignent certains auteurs, la commission d’infractions dans le cadre des méthodes particulières de recherche est parfois nécessaire. Toutefois, il convient de distinguer deux catégories de faits délictueux. Si la première catégorie ne soulève pas de problème car il s’agira principalement

hoofdzaak gaat om strafbare feiten die geen schade berokkenen aan de rechten van anderen, zoals het feit dat een politieambtenaar over valse identiteitspapieren beschikt, is de tweede categorie problematischer, om de volgende reden:

"... *elle rassemble toutes les infractions nécessaires pour atteindre les objectifs poursuivis par l'opération, telles que notamment l'intégration dans une organisation criminelle, la réalisation d'un pseudo-achat en pratiquant des achats-tests ou encore le démantèlement d'une association de malfaiteurs en fournissant à ses membres les moyens en vue de réaliser leurs activités*."[34].

Het ontworpen artikel 47*quinquies* van het Wetboek van Strafvordering heeft zijnerzijds betrekking op elke soort van strafbaar feit. In dat verband wordt in de memorie van toelichting gesteld dat zulks met verschillende redenen te maken heeft.

"Vooreerst geeft de bevoegde magistraat uitdrukkelijk aan welke misdrijven volgens hem toelaatbaar zijn, door deze, in de mate van het mogelijke en het voorzienbare, in een afzonderlijke en schriftelijke beschikking op te nemen. Een tweede reden is dat het praktisch eenvoudigweg niet mogelijk is alle situaties te voorzien, waarin de politieambtenaar onverwachts bij het plegen van strafbare feiten kan betrokken worden. Hieruit volgt, *a fortiori*, dat het dan ook onbegonnen werk is al deze misdrijven in een exhaustieve lijst te vatten. Een derde reden is tenslotte dat het uitsluiten van bepaalde misdrijven, bijvoorbeeld elk geweldsdelict, onmiddellijk als gevolg zou hebben dat criminele organisaties de proef op de som (in Nederland genoemd: 'het verschaffen van een pasklare lakmoestest") zouden nemen ter controle van de intenties van toetredende leden. Het zou alsdan, in het voorbeeld, volstaan de infiltrant te vragen ten opzichte van een derde persoon één of andere daad van geweld te gebruiken, opdat deze dit zou moeten weigeren, a-typisch gedrag zou beginnen vertonen en uiteindelijk door de mand zou vallen.'[35]

Het lijkt bezwaarlijk toelaatbaar dat de Staat zijn eigen ambtenaren zou kunnen toestaan bepaalde soorten strafbare feiten te begaan, terwijl krachtens inzonderheid de artikelen 2, 3 en 4 van het Verdrag tot bescherming van de rechten van de mens hij respectievelijk eenieders recht op leven moet beschermen, alsook een verbod moet stellen op foltering, onmenselijke of vernederende behandeling, slavernij en dwangarbeid. In de ontworpen tekst moet dus minstens gepreciseerd worden welke strafbare feiten nooit begaan mogen worden.

b) de zoëven gemaakte opmerking a), klemt des te meer wanneer het gaat om personen die niet de hoedanigheid hebben van politieambtenaar.

Volgens de bewoordingen van het ontworpen artikel 47*quinquies*, § 2, tweede lid, van het Wetboek van Strafvordering kan deze verschoningsgrond ook van toepassing zijn

d'infractions ne lésant pas les droits d'autrui, comme le fait pour le policier d'être titulaire de faux papiers d'identité, la seconde catégorie est plus problématique. En effet,

"... elle rassemble toutes les infractions nécessaires pour atteindre les objectifs poursuivis par l'opération, telles que notamment l'intégration dans une organisation criminelle, la réalisation d'un pseudo-achat en pratiquant des achats-tests ou encore le démantèlement d'une association de malfaiteurs en fournissant à ses membres les moyens en vue de réaliser leurs activités." [34].

L'article 47*quinquies*, en projet, du Code d'instruction criminelle vise quant à lui tout type d'infraction. A ce propos, l'exposé des motifs indique que cela tient à plusieurs raisons.

"Tout d'abord, le magistrat indique clairement les délits qui, selon lui, peuvent être autorisés, en les reprenant, dans la mesure du possible et pour autant que ceux-ci soient prévisibles, dans une disposition écrite et séparée. Une deuxième raison réside dans le fait qu'il est pratiquement impossible de prévoir toutes les situations dans lesquelles le fonctionnaire de police peut être amené à commettre inopinément des délits. Il s'ensuit, a fortiori, qu'il est pour ainsi dire impossible d'énumérer tous les délits dans une liste exhaustive. Une troisième raison tient au fait que l'exclusion de certains délits, par exemple, tout délit de violence, aurait immédiatement pour conséquence que des organisations criminelles seraient tentées de faire un test (aux Pays-Bas, cela s'appelle 'la mise à disposition d'un test à l'hélianthine sur mesure") pour jauger les intentions des nouveaux membres. Dans cette hypothèse, il suffirait alors de demander à l'infiltrant de perpétrer un acte de violence à l'égard d'un tiers pour que celui-ci soit contraint de le refuser, commencerait à manifester un comportement atypique et finirait par être découvert.' [35].

Il paraît difficilement admissible que l'État puisse autoriser ses agents à commettre certains types d'infractions, alors qu'en vertu notamment des articles 2, 3 et 4 de la Convention de sauvegarde des droits de l'homme, il doit respectivement protéger le droit à la vie de toute personne, interdire la torture, les traitements inhumains et dégradants ainsi que l'esclavage et le travail forcé. En conséquence, le texte en projet devrait, à tout le moins, préciser les infractions qui ne peuvent jamais être commises.

b) L'observation a) formulée ci-dessus s'impose avec d'autant plus de rigueur lorsqu'il s'agit de personnes n'ayant pas la qualité de fonctionnaires de police.

Par ailleurs, aux termes de l'article 47*quinquies*, § 2, alinéa 2, en projet, du Code d'instruction criminelle, cette cause d'excuse peut également s'appliquer

[34] *Voetnoot 30 van het geciteerde advies*: Ch. De Valkeneer, op. cit., blz. 459.

[35] *Voetnoot 31 van het geciteerde advies*: Zie de memorie van toelichting, blz. 18.

[34] *Note 29 de l'avis cité:* Ch. De Valkeneer, op. cit., p. 459.

[35] *Note 30 de l'avis cité:* Voir l'exposé des motifs, p. 18.

"... op de personen die aan de uitvoering van deze opdracht noodzakelijke en rechtstreekse hulp of bijstand hebben verleend en op de personen, bedoeld in artikel 47*octies*, § 1, tweede lid".

Dat betekent dat die verschoningsgrond eveneens zou kunnen worden aangevoerd door een persoon die geen politieambtenaar is, zoals een burger-deskundige of een informant, over wier rechtpositieregeling niets geweten is... Als het om een informant gaat die zelf strafbare feiten heeft begaan binnen het bestek van bijvoorbeeld zijn deelname aan een criminele organisatie, rijst de vraag of hij zich kan beroepen op die verschoningsgrond, waardoor hij gerechtelijk niet vervolgd zou kunnen worden, met dien verstande dat ervan uit mag worden gegaan dat de strafbare feiten die hij begaan heeft noodzakelijk waren voor de uitvoering van zijn opdracht.

De memorie van toelichting zou hierover duidelijker moeten zijn."[36]

Hoewel de tekst van artikel 47*quinquies* enigszins werd aangepast in het licht van deze opmerking, blijven een aantal van de erin opgenomen bedenkingen actueel.

25. In de memorie van toelichting wordt vooropgesteld dat voor de in het ontworpen artikel 46*sexies* van het Wetboek van Strafvordering opgenomen maatregel van infiltratie op het internet een eigen regime verantwoord is "aangezien de infiltratie op internet een minder verregaand karakter heeft dan de klassieke infiltratie, en aangezien de verschillende contacten gedurende de uitvoering van deze maatregel worden geregistreerd".

De vraag rijst evenwel of deze vrij algemene verantwoording alle verschillen tussen de beide regelingen kan verantwoorden. Zo is het niet duidelijk waarom de procureur des Konings, in tegenstelling tot wat het geval is voor de klassieke infiltratie, geen maatregelen kan nemen ter vrijwaring van de veiligheid en de fysieke, psychische en morele integriteit van de cyber-infiltrant (zie artikel 47*octies*, § 2, laatste lid, van het Wetboek van Strafvordering).

26. In het ontworpen artikel 46*sexies*, § 1, eerste lid, van het Wetboek van Strafvordering wordt aan de minister bevoegd voor justitie een delegatie toegekend om de politiediensten aan te wijzen die op het internet, desgevallend onder een fictieve identiteit, contact kunnen onderhouden met een of meerdere personen ten aanzien waarvan[37] er ernstige aanwijzingen zijn dat zij bepaalde strafbare feiten hebben gepleegd. Nog daargelaten dat de wetgever in beginsel niet vermag delegaties te verlenen aan een minister,[38] dient erop te worden gewezen dat het bepalen van welke politiediensten kunnen worden gemachtigd de in te voeren onderzoeksmaatregel uit te voeren, een essentieel element van de regeling is dat door de wetgever zelf dient te worden vastgesteld op grond van het in artikel 12, tweede lid, van de Grondwet vervatte legaliteitsbeginsel, dat ook voor het opsporingsonderzoek geldt.[39]

[36] Adv.RvS 32 673/2, *l.c.*, 140-142. Zie evenwel de voorafgaande opmerking uit dat advies.
[37] De woorden "ten aanzien" ontbreken in de Nederlandse tekst.
[38] Zie opmerking 20.
[39] GwH 21 december 2004, nr. 202/2004, B.4.2.

"... aux personnes qui ont fourni directement une aide ou une assistance nécessaire à l'exécution de cette mission ainsi qu'aux personnes visées à l'article 47*octies*, § 1er, alinéa 2".

Ceci implique que la cause d'excuse pourrait également être invoquée par une personne n'ayant pas la qualité de fonctionnaire de police, comme l'expert civil ou l'indicateur dont on ignore tout du statut... S'agissant d'un indicateur ayant lui-même commis des infractions, dans le cadre par exemple de sa participation à une organisation criminelle, la question se pose de savoir s'il pourra se prévaloir de cette cause d'excuse le mettant ainsi à l'abri de toute poursuite judiciaire, étant entendu que l'on puisse considérer que les infractions qu'il a commises soient nécessaires à l'exécution de la mission?

L'exposé des motifs gagnerait à être plus clair sur ce point" [36].

Bien que le texte de l'article 47*quinquies* ait été quelque peu adapté à la lumière de cette observation, un certain nombre de considérations qui y figurent restent d'actualité.

25. L'exposé des motifs indique qu'un régime propre est justifié pour la mesure d'infiltration sur Internet inscrite à l'article 46*sexies* en projet du Code d'instruction criminelle, "[é]tant donné que l'infiltration sur Internet a un caractère moins intrusif que l'infiltration "classique" et que les différents contacts durant l'exécution de cette mesure sont enregistrés".

La question se pose toutefois de savoir si cette justification relativement générale peut légitimer toutes les différences entre les deux régimes. Ainsi, on n'aperçoit pas clairement pourquoi le procureur du Roi, contrairement à ce qui est le cas pour l'infiltration classique, ne peut pas prendre des mesures en vue de garantir la sécurité, ainsi que l'intégrité physique, psychique et morale du cyberinfiltrant (voir l'article 47*octies*, § 2, dernier alinéa, du Code d'instruction criminelle).

26. L'article 46*sexies*, § 1er, alinéa 1er, en projet, du Code d'instruction criminelle habilite le ministre qui a la Justice dans ses attributions à désigner les services de police qui entretiennent sur Internet, le cas échéant sous une identité fictive, des contacts avec une ou plusieurs personnes concernant lesquelles [37] il existe des indices sérieux qu'elles ont commis certaines infractions. Outre le fait que le législateur ne peut en principe pas accorder de délégations à un ministre [38], il faut souligner que la désignation des services de police habilités à mettre en œuvre la mesure d'enquête envisagée constitue un élément essentiel du régime qui doit être fixé par le législateur même en vertu du principe de légalité inscrit à l'article 12, alinéa 2, de la Constitution qui s'applique également à l'information [39].

[36] Avis C.E. 32 673/2, *l.c.*, 140-142. Voir toutefois l'observation préalable de cet avis.
[37] Il manque les mots "ten aanzien" dans le texte néerlandais.
[38] Voir l'observation 20.
[39] C.C., 21 décembre 2004, n° 202/2004, B.4.2.

27. De stellers van het ontwerp dienen na te gaan of het niet mogelijk is het in het ontworpen artikel 46*sexies*, § 1, tweede lid, van het Wetboek van Strafvordering opgenomen begrip "uitzonderlijke omstandigheden" nader te omschrijven en die bepaling overeenkomstig aan te vullen.

28. De gemachtigde verklaarde dat de strafbare feiten tot het plegen waarvan de betrokken politiediensten met toepassing van het aan te nemen artikel 46*sexies*, § 3, van het Wetboek van Strafvordering zouden kunnen worden gemachtigd, niet noodzakelijkerwijze beperkt blijven tot strafbare feiten die worden gepleegd in cyberspace.

De verhouding tussen die bepaling en de artikelen 47*quinquies* en 47*octies* van het Wetboek van Strafvordering dient dan te worden uitgeklaard.

29. Luidens het ontworpen artikel 46*sexies,* § 3, vijfde lid, van het Wetboek van Strafvordering melden de betrokken politieambtenaren schriftelijk *en vóór de uitvoering van de maatregel* aan de procureur des Konings de misdrijven die zij of diegenen die hen bijstaan op grond van het ontworpen artikel 46*sexies*, § 1, tweede lid, van dat wetboek, voornemens zijn te plegen, waarop luidens het ontworpen artikel 46*sexies,* § 3, zevende lid, de procureur des Konings erover beslist welke misdrijven kunnen worden gepleegd.[40] In het ontworpen artikel 46*sexies*, § 3, zesde lid, van het Wetboek van Strafvordering wordt erin evenwel, zonder dat enig criterium wordt bepaald, voorzien in de hypothese dat "de voorafgaande kennisgeving niet kon gebeuren", in welk geval de loutere melding van het plegen van de misdrijven volstaat. Daardoor dreigt de voorafgaande controle door de procureur des Konings te worden uitgehold. Hierover ondervraagd, verklaarde de gemachtigde wat volgt:

"Ons inziens holt deze bepaling het toezicht van de procureur des Konings niet uit.

Vooreerst is de gehele regeling omtrent het plegen van misdrijven door politieambtenaren quasi identiek aan de regeling die vandaag reeds geldt bij toepassing van de bijzondere opsporingsmethoden (art. 47*quinquies* Sv.).

Het voorzien van de mogelijkheid om strafbare feiten te plegen zonder voorafgaande machtiging van de procureur des Konings is in dezelfde mate noodzakelijk als bij de "klassieke" infiltratie. De memorie van toelichting bij de "BOM-wet" van 6 januari 2003 motiveert dit als volgt:

'Het kan niet worden uitgesloten dat de politieambtenaar, tijdens de uitvoering van de bijzondere opsporingsmethoden, geconfronteerd wordt met uitzonderlijke omstandigheden, die hem er toe nopen strafbare handelingen te stellen, die niet te voorzien waren en niet op voorhand met de magistraat konden worden doorgesproken. In sommige gevallen bestaat nog de mogelijkheid om, alvorens de strafbare feiten daadwerkelijk te stellen, mondeling de magistraat in kennis te stellen. In andere gevallen is zelfs dit onmogelijk.

[40] Een gelijkaardige bepaling komt nu reeds voor in artikel 47*quinquies*, § 3, tweede lid, van het Wetboek van Strafvordering.

27. Les auteurs du projet vérifieront s'il n'est pas possible de préciser la notion de "circonstances exceptionnelles" figurant à l'article 46*sexies*, § 1er, alinéa 1er, en projet, du Code d'instruction criminelle et de la compléter en conséquence.

28. Le délégué a déclaré que les infractions pouvant donner lieu à l'habilitation des services de police concernés en application de l'article 46*sexies*, § 3, envisagé du Code d'instruction criminelle ne se limitent pas nécessairement aux infractions commises dans le cyberespace.

Le rapport entre cette disposition et les articles 47*quinquies* et 47*octies* du Code d'instruction criminelle devra donc être clarifié.

29. Aux termes de l'article 46*sexies*, § 3, alinéa 5, en projet, du Code d'instruction criminelle, les fonctionnaires de police communiquent, par écrit et préalablement à l'exécution de la mesure, au procureur du Roi les infractions qu'eux-mêmes ou les personnes qui les assistent en vertu de l'article 46*sexies*, § 1er, alinéa 2, en projet, de ce code ont l'intention de commettre, à la suite de quoi le procureur du Roi décide, selon l'article 46*sexies*, § 3, alinéa 7, en projet, quelles infractions peuvent être commises [40]. Cependant, l'article 46*sexies*, § 3, alinéa 6, en projet, du Code d'instruction criminelle prévoit, sans fixer aucun critère, l'hypothèse où la "notification préalable n'a pas pu avoir lieu", auquel cas il suffit de mentionner la commission des infractions. Le contrôle préalable par le procureur du Roi risque dès lors d'être vidé de toute substance. Interrogé à ce sujet, le délégué a déclaré ce qui suit:

"*Ons inziens holt deze bepaling het toezicht van de procureur des Konings niet uit.*

Vooreerst is de gehele regeling omtrent het plegen van misdrijven door politieambtenaren quasi identiek aan de regeling die vandaag reeds geldt bij toepassing van de bijzondere opsporingsmethoden (art. 47quinquies Sv.).

Het voorzien van de mogelijkheid om strafbare feiten te plegen zonder voorafgaande machtiging van de procureur des Konings is in dezelfde mate noodzakelijk als bij de "klassieke" infiltratie. De memorie van toelichting bij de "BOM-wet" van 6 januari 2003 motiveert dit als volgt:

'Het kan niet worden uitgesloten dat de politieambtenaar, tijdens de uitvoering van de bijzondere opsporingsmethoden, geconfronteerd wordt met uitzonderlijke omstandigheden, die hem er toe nopen strafbare handelingen te stellen, die niet te voorzien waren en niet op voorhand met de magistraat konden worden doorgesproken. In sommige gevallen bestaat nog de mogelijkheid om, alvorens de strafbare feiten daadwerkelijk te stellen, mondeling de magistraat in kennis te stellen. In andere gevallen is zelfs dit onmogelijk.

[40] Une disposition analogue figure déjà à l'article 47*quinquies*, § 3, alinéa 2, du Code d'instruction criminelle.

Wederom kan gedacht worden aan de infiltrant. Bij infiltratie is niet steeds te voorzien welke handelingen nodig zullen zijn, wil de infiltrant zich ten behoeve van zijn opdracht geloofwaardig maken als deelnemer aan een criminele organisatie. Zijn veiligheid kan op het spel staan, als hij (onverwachte) opdrachten weigert die een deelnemer in de organisatie in zijn positie niet behoort te weigeren (…) Het volstaat dat hij onverwacht door de criminele organisatie wordt uitgenodigd een verdachte transactie of een strafbaar feit daadwerkelijk zelf bij te wonen, opdat hij zich in een positie van potentieel mededaderschap of medeplichtigheid aan misdrijven bevindt. In dergelijke gevallen is het onvermijdbaar dat de politieambtenaar strafbare feiten pleegt' (*Parl.St.* Kamer 2001-2002, 50-1688/001, p. 26).

Bovendien behoudt de procureur des Konings steeds zijn recht om het gepleegde misdrijf *a posteriori* te toetsen:

"Het komt de magistraat dan toe, weliswaar achteraf, een oordeel te vellen over de handelingen en gedragingen van de politieambtenaar en deze af te toetsen aan de situatie, zoals zij zich heeft voorgedaan en waarin de politieambtenaar, soms in een fractie van tijd, tot het nemen van een beslissing werd gedwongen. Ook hier zal de magistraat de gepleegde strafbare feiten beoordelen in het licht van het welslagen van de operatie en de veiligheid van de politieambtenaar of andere bij de operatie betrokken personen. Mocht de magistraat van oordeel zijn dat de gepleegde strafbare feiten het kader van de opdracht of van de bijzondere opsporingsmethoden volledig te buiten gaan of werkelijk onrechtmatig en onaanvaardbaar zijn, zal hij hieraan het strafrechtelijk gevolg, dat hij passend acht, verlenen" (*Parl.St*. Kamer 2001-2002, 50-1688/001, p. 26-27)."

Het verdient aanbeveling dat de in het antwoord van de gemachtigde vermelde elementen b*eter* tot uiting worden gebracht in de tekst van het ontworpen artikel 46*sexies,* § 3 (en in artikel 47*quinquies*, §§ 2 en 3) van het Wetboek van Strafvordering.

30. In de laatste zin van het ontworpen artikel 46*sexies*, § 3, zevende lid, van het Wetboek van Strafvordering wordt bepaald dat de inhoud van het erin bedoelde dossier onder het beroepsgeheim valt. In die zin wordt slechts een evidentie vertolkt, zodat hij b*eter* wordt weggelaten, temeer nu erdoor twijfel zou kunnen worden gezaaid over de juiste omvang van het beroepsgeheim.

Artikel 11

31. Wat betreft de uitbreiding van het toepassingsgebied van artikel 56*bis* van het Wetboek van Strafvordering kan worden verwezen naar hetgeen de Raad van State daaromtrent, wat betreft de bijzondere opsporingsmethodes, in advies 32 673/2 heeft opgemerkt *sub* V.[41]

32. Luidens de aan artikel 56*bis*, vierde lid, van het Wetboek van Strafvordering toe te voegen zin zijn de stafhouder of de vertegenwoordiger van de provinciale orde van

[41] *L.c.,* 146-150.

Wederom kan gedacht worden aan de infiltrant. Bij infiltratie is niet steeds te voorzien welke handelingen nodig zullen zijn, wil de infiltrant zich ten behoeve van zijn opdracht geloofwaardig maken als deelnemer aan een criminele organisatie. Zijn veiligheid kan op het spel staan, als hij (onverwachte) opdrachten weigert die een deelnemer in de organisatie in zijn positie niet behoort te weigeren (…) Het volstaat dat hij onverwacht door de criminele organisatie wordt uitgenodigd een verdachte transactie of een strafbaar feit daadwerkelijk zelf bij te wonen, opdat hij zich in een positie van potentieel mededaderschap of medeplichtigheid aan misdrijven bevindt. In dergelijke gevallen is het onvermijdbaar dat de politieambtenaar strafbare feiten pleegt' (Parl. St. Kamer 2001-2002, 50-1688/001, p. 26).

Bovendien behoudt de procureur des Konings steeds zijn recht om het gepleegde misdrijf a posteriori te toetsen:

"Het komt de magistraat dan toe, weliswaar achteraf, een oordeel te vellen over de handelingen en gedragingen van de politieambtenaar en deze af te toetsen aan de situatie, zoals zij zich heeft voorgedaan en waarin de politieambtenaar, soms in een fractie van tijd, tot het nemen van een beslissing werd gedwongen. Ook hier zal de magistraat de gepleegde strafbare feiten beoordelen in het licht van het welslagen van de operatie en de veiligheid van de politieambtenaar of andere bij de operatie betrokken personen. Mocht de magistraat van oordeel zijn dat de gepleegde strafbare feiten het kader van de opdracht of van de bijzondere opsporingsmethoden volledig te buiten gaan of werkelijk onrechtmatig en onaanvaardbaar zijn, zal hij hieraan het strafrechtelijk gevolg, dat hij passend acht, verlenen" (Parl.St. Kamer 2001-2002, 50-1688/001, p. 26-27)".

Il est recommandé de mieux exprimer les éléments mentionnés dans la réponse du délégué dans le texte de l'article 46*sexies*, § 3, en projet (et de l'article 47*quinquies*, §§ 2 et 3) du Code d'instruction criminelle.

30. La dernière phrase de l'article 46*sexies*, § 3, alinéa 7, en projet, du Code d'instruction criminelle dispose que le contenu du dossier qui y est visé est couvert par le secret professionnel. Cette phrase ne fait que traduire une évidence, si bien qu'il serait préférable de l'omettre, d'autant qu'elle pourrait semer le doute quant à la portée exacte du secret professionnel.

Article 11

31. En ce qui concerne l'extension du champ d'application de l'article 56*bis* du Code d'instruction criminelle, l'on peut se référer à l'observation formulée à ce sujet, en ce qui concerne les méthodes particulières de recherche, par le Conseil d'État dans son avis 32 673/2, point V [41].

32. Aux termes de la phrase à ajouter à l'article 56*bis*, alinéa 4, du Code d'instruction criminelle, le bâtonnier ou le représentant de l'ordre provincial des médecins est tenu

[41] *L.c.*, 146-150.

geneesheren tot geheimhouding verplicht wanneer zij op de hoogte worden gebracht van de in artikel 56*bis*, derde lid, genomen maatregelen en wordt de miskenning van deze plicht gestraft overeenkomstig artikel 458 van het Strafwetboek. De genoemde personen lijken evenwel reeds onder het toepassingsgebied op zich van dat laatste artikel te vallen, zodat de vraag rijst of het niet overbodig is dat artikel nogmaals van toepassing te maken. Ook op andere plaatsen in het Wetboek van Strafvordering komt zulk een bepaling voor, terwijl erin ook de meer algemene artikelen 28*quinquies*, § 1, tweede lid, en 57, § 1, tweede lid, zijn opgenomen. De onderlinge verhouding tussen de laatstgenoemde bepalingen, de specifieke bepalingen inzake beroepsgeheim die zijn opgenomen in het Wetboek van Strafvordering en artikel 458 van het Strafwetboek verdient dan ook een verder onderzoek.

Eenzelfde opmerking geldt ten aanzien van artikel 12, 2°, van het ontwerp.

Artikel 12

33. De gemachtigde verklaarde het volgende omtrent het ontworpen artikel 88*bis*, § 1, zesde lid, van het Wetboek van Strafvordering:

"De voorgestelde wijziging van dit lid bestaat enkel in de toevoeging van artikel 434 Sw. Dit artikel wordt ook toegevoegd in artikel 90ter, § 5 Sv. De motivering bij die laatste toevoeging is opgenomen in de memorie van toelichting, p. 63: "Toevoeging van artikel 434 Sw. (wederrechtelijke vrijheidsberoving). Aangezien de toepassing van de maatregel van artikel 90ter, § 1, in de context van wederrechtelijke vrijheidsberoving vaak noodzakelijk is binnen een zeer korte tijdspanne, wordt de procureur des Konings de mogelijkheid gegeven om deze maatregel te bevelen wanneer het gaat om ontdekking op heterdaad". De toevoeging van artikel 434 Sw. in artikel 88bis, § 1, zesde lid Sv. heeft tot doel de procureur des Konings toe te laten de maatregel van artikel 88*bis* te bevelen en de verantwoordelijkheid voor de uitvoering ervan te dragen zolang de heterdaadsituatie duurt. Wij zullen deze motivering opnemen in de memorie bij artikel 88*bis*."

Artikel 14

34. Artikel 14, 1°, van het ontwerp strekt onder meer tot vervanging van het woord "personen" door de woorden "aan eenieder" in artikel 88*quater*, § 1, eerste zin, van het Wetboek van Strafvordering. De gemachtigde verklaarde hieromtrent wat volgt:

"Voor wat betreft artikel 14 (dat handelt over artikel 88*quater* Sv.): het voorontwerp spreekt over "eenieder", dus ook rechtspersonen worden beoogd. Voor het overige wijzigt het voorontwerp niets aan het toepassingsgebied van dit artikel zoals verduidelijkt in de memorie van toelichting bij de wet inzake informaticacriminaliteit: "In antwoord op de Raad van State moet gesteld worden dat de kring van personen die geviseerd worden door artikel 88*quater* niet in abstracto kan worden omschreven: het kan gaan om importeurs/verdelers van computers of software, "*trusted third parties*",

au secret lorsqu'il est informé des mesures prises à l'article 56*bis*, alinéa 3, et la méconnaissance de cette obligation est punie conformément à l'article 458 du Code pénal. Toutefois, les personnes visées semblent en soi déjà relever du champ d'application de ce dernier article, de sorte que la question se pose de savoir s'il n'est pas superflu de rendre une nouvelle fois cet article applicable. Une disposition analogue figure également en d'autres endroits du Code d'instruction criminelle, alors que celui-ci comporte déjà les articles 28*quinquies*, § 1er, alinéa 2, et 57, § 1er, alinéa 2, plus généraux. Il est dès lors recommandé d'examiner plus avant le rapport entre ces dernières dispositions, les dispositions spécifiques relatives au secret professionnel inscrites dans le Code d'instruction criminelle ainsi que l'article 458 du Code pénal.

La même observation peut être formulée à l'égard de l'article 12, 2°, du projet.

Article 12

33. Au sujet de l'article 88*bis*, § 1er, alinéa 6, en projet, du Code d'instruction criminelle, le délégué a déclaré ce qui suit:

"De voorgestelde wijziging van dit lid bestaat enkel in de toevoeging van artikel 434 Sw. Dit artikel wordt ook toegevoegd in artikel 90ter, § 5 Sv. De motivering bij die laatste toevoeging is opgenomen in de memorie van toelichting, p. 63: "Toevoeging van artikel 434 Sw. (wederrechtelijke vrijheidsberoving). Aangezien de toepassing van de maatregel van artikel 90ter, § 1, in de context van wederrechtelijke vrijheidsberoving vaak noodzakelijk is binnen een zeer korte tijdspanne, wordt de procureur des Konings de mogelijkheid gegeven om deze maatregel te bevelen wanneer het gaat om ontdekking op heterdaad". De toevoeging van artikel 434 Sw. in artikel 88bis, § 1, zesde lid Sv. heeft tot doel de procureur des Konings toe te laten de maatregel van artikel 88bis te bevelen en de verantwoordelijkheid voor de uitvoering ervan te dragen zolang de heterdaadsituatie duurt. Wij zullen deze motivering opnemen in de memorie bij artikel 88bis".

Article 14

34. L'article 14, 1°, du projet a entre autres pour objet de remplacer les mots "aux personnes" par les mots "à quiconque" à l'article 88*quater*, § 1er, première phrase, du Code d'instruction criminelle. À ce propos, le délégué a déclaré ce qui suit:

"Voor wat betreft artikel 14 (dat handelt over artikel 88quater Sv.): het voorontwerp spreekt over "eenieder", dus ook rechtspersonen worden beoogd. Voor het overige wijzigt het voorontwerp niets aan het toepassingsgebied van dit artikel zoals verduidelijkt in de memorie van toelichting bij de wet inzake informaticacriminaliteit: "In antwoord op de Raad van State moet gesteld worden dat de kring van personen die geviseerd worden door artikel 88quater niet in abstracto kan worden omschreven: het kan gaan om importeurs/verdelers van computers of software, 'trusted third parties",

dienstenverstrekkers, operatoren, bedrijfsingenieurs die een specifieke informaticaconfiguratie hebben uitgewerkt, beveiligingsspecialisten, … De onderzoeksrechter zal dit geval per geval moeten nagaan. Bovendien gaat het uiteraard slechts om een inspanningsverbintenis: men kan immers niet meer van iemand verlangen dan hij zelf vermag' (*Parl. St*. Kamer 1992-2000, 50-213/001, p. 27).

Voor wat betreft artikel 18 (dat handelt over artikel 90*quater* Sv.): het voorontwerp spreekt in artikel 90*quater*, § 2 enkel over operatoren en dienstenverstrekkers. In § 4 gaat het over "personen", dus ook rechtspersonen worden beoogd. Voor het overige geldt hetzelfde als hierboven gesteld.

Voor wat betreft artikel 28 (dat handelt over artikel 464/25 Sv.): ook hier betreft het slechts operatoren en dienstenverstrekkers."

Het verdient aanbeveling deze verduidelijking in de memorie van toelichting op te nemen.

Artikel 17

35. In het ontworpen artikel 90*ter*, § 2, 36°, van het Wetboek van Strafvordering (artikel 17, 2°, van het ontwerp) vervange men de woorden "het Vlaams Parlement" door de woorden "het Vlaamse Gewest".

Artikel 21

36. De stellers van het ontwerp dienen na te gaan of niet het best een termijn wordt bepaald waarbinnen de in het ontworpen artikel 90*septies*, § 3, van het Wetboek van Strafvordering bedoelde gegevens dienen te worden vernietigd.

37. Er dient, minstens in de memorie van toelichting, te worden verduidelijkt wat wordt bedoeld met de in het ontworpen artikel 90*septies,* § 3, tweede lid, van het Wetboek van Strafvordering bedoelde begrip "beheersredenen".

Artikel 22

38. De gemachtigde verschafte de volgende toelichting bij het ontworpen 90*octies*, § 3, derde lid, van het Wetboek van Strafvordering:

"Paragraaf 3, laatste lid betreft specifiek de gegevens die onder het beroepsgeheim vallen. Ter bescherming van dit beroepsgeheim worden de gegevens afzonderlijk ter griffie bewaard. Op die manier kan achteraf in voorkomend geval nog toepassing worden gemaakt van artikel 90*septies*, § 6, tweede lid Sv. (m.b.t. het verzoek tot raadpleging of bijkomende overschrijving van de "andere bestanden of gegevens")."

Die uitleg zou in de memorie van toelichting kunnen worden opgenomen.

dienstenverstrekkers, operatoren, bedrijfsingenieurs die een specifieke informaticaconfiguratie hebben uitgewerkt, beveiligingsspecialisten, … De onderzoeksrechter zal dit geval per geval moeten nagaan. Bovendien gaat het uiteraard slechts om een inspanningsverbintenis: men kan immers niet meer van iemand verlangen dan hij zelf vermag' (Parl. St. Kamer 1992-2000, 50-213/001, p. 27).

Voor wat betreft artikel 18 (dat handelt over artikel 90quater Sv.): het voorontwerp spreekt in artikel 90quater, § 2 enkel over operatoren en dienstenverstrekkers. In § 4 gaat het over "personen", dus ook rechtspersonen worden beoogd. Voor het overige geldt hetzelfde als hierboven gesteld.

Voor wat betreft artikel 28 (dat handelt over artikel 464/25 Sv.): ook hier betreft het slechts operatoren en dienstenverstrekkers".

Il est recommandé d'insérer cette précision dans l'exposé des motifs.

Article 17

35. À l'article 90*ter*, § 2, 36°, en projet, du Code d'instruction criminelle (article 17, 2°, du projet), on remplacera les mots "du parlement flamand" par les mots "de la Région flamande".

Article 21

36. Les auteurs du projet vérifieront s'il n'est pas préférable de fixer un délai dans lequel les données visées à l'article 90*septies*, § 3, en projet, du Code d'instruction criminelle devront être détruites.

37. Il convient de préciser, au moins dans l'exposé des motifs, ce qu'il faut entendre par la notion de "raisons de gestion" visée à l'article 90*septies*, § 3, alinéa 2, en projet, du Code d'instruction criminelle.

Article 22

38. Le délégué a fourni l'explication suivante concernant l'article 90*octies*, § 3, alinéa 3, en projet, du Code d'instruction criminelle:

"Paragraaf 3, laatste lid betreft specifiek de gegevens die onder het beroepsgeheim vallen. Ter bescherming van dit beroepsgeheim worden de gegevens afzonderlijk ter griffie bewaard. Op die manier kan achteraf in voorkomend geval nog toepassing worden gemaakt van artikel 90septies, § 6, tweede lid Sv. (m.b.t. het verzoek tot raadpleging of bijkomende overschrijving van de "andere bestanden of gegevens")".

Cette explication devrait être reproduite dans l'exposé des motifs.

Artikel 28

39. De gemachtigde verklaarde dat in artikel 28, 1°, van het ontwerp een vervanging, en niet een invoeging van woorden wordt beoogd en dat het ontwerp op dit punt zal worden aangepast.

De griffier, *De voorzitter,*

Annemie GOOSSENS Jo BAERT

Article 28

39. Le délégué a fait savoir qu'à l'article 28, 1°, du projet, l'intention était de procéder à un remplacement, et non à une insertion de mots, et que le projet sera adapté sur ce point.

Le greffier, *Le président,*

Annemie GOOSSENS Jo BAERT

WETSONTWERP

FILIP,

KONING DER BELGEN,

Aan allen die nu zijn en hierna wezen zullen,
Onze Groet.

op de voordracht van onze minister van Justitie,

HEBBEN WIJ BESLOTEN EN BESLUITEN WIJ:

De minister van Justitie is ermee belast het ontwerp van wet, waarvan de tekst hierna volgt, in Onze naam voor te leggen en bij de Kamer van volksvertegenwoordigers in te dienen:

TITEL 1

Algemene bepaling

Artikel 1

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

TITEL 2

Bepalingen tot wijziging van het Wetboek van Strafvordering

Artikel 2

In artikel 39*bis* van het Wetboek van Strafvordering, ingevoegd bij wet van 28 november 2000 en gewijzigd bij wet van 6 juni 2010, worden de volgende wijzigingen aangebracht:

1° In paragraaf 1 worden de woorden “of een deel ervan” ingevoegd tussen de woorden “een informaticasysteem” en de woorden “opgeslagen gegevens.”;

2° paragraaf 2 wordt vervangen als volgt:

“§ 2. Tot de zoeking in een informaticasysteem of een deel ervan dat in beslag genomen is, kan beslist worden door een officier van gerechtelijke politie.

Onverminderd het vorige lid, kan de procureur des Konings een zoeking bevelen in een informaticasysteem of een deel ervan dat door hem in beslag kan worden genomen.

PROJET DE LOI

PHILIPPE,

ROI DES BELGES,

À tous, présents et à venir,
SALUT.

sur la proposition de notre ministre de la Justice,

NOUS AVONS ARRÊTÉ ET ARRÊTONS:

Le ministre de la Justice est chargé de présenter en Notre nom et de déposer à la Chambre des représentants le projet de loi dont la teneur suit:

TITRE 1ER

Disposition générale

Article 1er

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

TITRE 2

Dispositions modifiant le Code d’Instruction criminelle

Article 2

A l’article 39*bis* du Code d’instruction criminelle, inséré par la loi du 28 novembre 2000 et modifié par la loi du 6 juin 2010, les modifications suivantes sont apportées:

1° Le paragraphe 1er est complété par les mots “ou une partie de celui-ci.”;

2° le paragraphe 2 est remplacé par ce qui suit:

“§ 2. La recherche dans un système informatique ou une partie de celui-ci qui a été saisi, peut être décidée par un officier de police judiciaire.

Sans préjudice de l’alinéa précédent, le procureur du Roi peut ordonner une recherche dans un système informatique ou une partie de celui-ci qui peut être saisi par lui.

De zoekingen bedoeld in het eerste en het tweede lid kunnen zich enkel uitstrekken tot de gegevens die opgeslagen zijn op het informaticasysteem dat, respectievelijk, in beslag genomen is of in beslag kan worden genomen.";

3° Paragraaf 3 wordt vervangen als volgt:

"§ 3. De procureur des Konings kan de zoeking in een informaticasysteem of een deel ervan, aangevat op grond van § 2, uitbreiden naar een informaticasysteem of een deel daarvan dat zich op een andere plaats bevindt dan daar waar de zoeking plaatsvindt:

— indien deze uitbreiding noodzakelijk is om de waarheid aan het licht te brengen ten aanzien van het misdrijf dat het voorwerp uitmaakt van de zoeking; en

— indien andere maatregelen disproportioneel zouden zijn, of indien er een risico bestaat dat zonder deze uitbreiding bewijselementen verloren gaan.

De uitbreiding van de zoeking in een informaticasysteem mag zich niet verder uitstrekken dan tot de informaticasystemen of de delen daarvan waartoe de personen die gerechtigd zijn het onderzochte informaticasysteem te gebruiken, in het bijzonder toegang hebben.

Inzake de door uitbreiding van de zoeking in een informaticasysteem aangetroffen gegevens, die nuttig zijn voor dezelfde doeleinden als de inbeslagneming, wordt gehandeld zoals bepaald in § 6.

Wanneer blijkt dat deze gegevens zich niet op het grondgebied van het Rijk bevinden, worden ze enkel gekopieerd. In dat geval deelt de procureur des Konings dit onverwijld mee aan de Federale Overheidsdienst Justitie, dat de bevoegde overheid van de betrokken Staat hiervan op de hoogte brengt, indien deze redelijkerwijze kan worden bepaald.

In geval van uiterst dringende noodzakelijkheid of in geval van heterdaad kan de procureur des Konings de uitbreiding van de zoeking bedoeld in het eerste lid mondeling bevelen. Dit bevel wordt zo spoedig mogelijk schriftelijk bevestigd, met vermelding van de heterdaadsituatie of van de redenen van de uiterst dringende noodzakelijkheid.";

4° paragraaf 4 wordt vervangen als volgt:

"§ 4. Enkel de onderzoeksrechter kan een andere zoeking bevelen in een informaticasysteem of een deel ervan dan de zoekingen voorzien in de paragrafen 2 en 3:

Les recherches visées aux alinéas 1 et 2 peuvent uniquement s'étendre aux données sauvegardées dans un système informatique qui est soit saisi, soit susceptible d'être saisi.";

3° Le paragraphe 3 est remplacé par ce qui suit:

"§ 3. Le procureur du Roi peut étendre la recherche dans un système informatique ou une partie de celui-ci, entamée sur la base du § 2, vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée:

— si cette extension est nécessaire pour la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche; et

— si d'autres mesures seraient disproportionnées, ou s'il existe un risque que, sans cette extension, des éléments de preuve soient perdus.

L'extension de la recherche dans un système informatique ne peut pas excéder les systèmes informatiques ou les parties de tels systèmes auxquels les personnes autorisées à utiliser le système informatique qui fait l'objet de la mesure ont spécifiquement accès.

En ce qui concerne les données recueillies par l'extension de la recherche dans un système informatique, qui sont utiles pour les mêmes finalités que celles prévues pour la saisie, les règles prévues au § 6 s'appliquent.

Lorsqu'il s'avère que ces données ne se trouvent pas sur le territoire du Royaume, elles peuvent seulement être copiées. Dans ce cas, le procureur du Roi communique sans délai cette information au Service public fédéral Justice, qui en informe les autorités compétentes de l'état concerné, si celui-ci peut raisonnablement être déterminée.

En cas d'extrême urgence ou de flagrant délit, le procureur du Roi peut ordonner verbalement l'extension de la recherche visée à l'alinéa 1er. Cet ordre est confirmé par écrit dans les meilleurs délais, avec mention du flagrant délit ou des motifs de l'extrême urgence.";

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

"§ 4. Seul le juge d'instruction peut ordonner une recherche dans un système informatique ou une partie de celui-ci autre que les recherches visées aux paragraphes 2 et 3:

— indien deze zoeking noodzakelijk is om de waarheid aan het licht te brengen ten aanzien van het misdrijf dat het voorwerp uitmaakt van de zoeking; en

— indien andere maatregelen disproportioneel zouden zijn, of indien er een risico bestaat dat zonder deze zoeking bewijselementen verloren gaan.

In geval van uiterst dringende noodzakelijkheid kan de onderzoeksrechter de uitbreiding van de zoeking bedoeld in het eerste lid mondeling bevelen. Dit bevel wordt zo spoedig mogelijk schriftelijk bevestigd, met vermelding van de heterdaadsituatie of van de redenen van de uiterst dringende noodzakelijkheid.";

5° het artikel wordt aangevuld met de paragrafen 5, 6, 7 en 8, luidende:

"§ 5. Teneinde de maatregelen bedoeld in dit artikel mogelijk te maken, kan de procureur des Konings of de onderzoeksrechter bevelen om, te allen tijde, ook zonder de toestemming van hetzij de eigenaar of zijn rechthebbende, hetzij de gebruiker:

— elke beveiliging van de betrokken informaticasystemen tijdelijk op te heffen, desgevallend met behulp van technische hulpmiddelen, valse signalen, valse sleutels of valse hoedanigheden;

— technische middelen in de betrokken informaticasystemen aan te brengen teneinde de door dat systeem opgeslagen, verwerkte of doorgestuurde gegevens te ontcijferen en te decoderen.

Evenwel kan enkel de onderzoeksrechter deze tijdelijke opheffing van de beveiliging of deze aanbrenging van technische middelen bevelen wanneer dit in het bijzonder noodzakelijk is voor de toepassing van paragraaf 3.

§ 6. Indien in de betrokken informaticasystemen opgeslagen gegevens aangetroffen worden die nuttig zijn voor dezelfde doeleinden als de inbeslagneming, maar de inbeslagneming van de drager daarvan evenwel niet wenselijk is, worden deze gegevens, evenals de gegevens noodzakelijk om deze te kunnen verstaan, gekopieerd op dragers, die toebehoren aan de overheid. In geval van dringendheid of om technische redenen, kan gebruik gemaakt worden van dragers, die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken.

Bovendien worden passende technische middelen aangewend om de toegang tot deze gegevens in het informaticasysteem, evenals tot de kopieën daarvan die ter beschikking staan van personen die gerechtigd zijn

— si cette recherche est nécessaire pour la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche; et

— si d'autres mesures seraient disproportionnées, ou s'il existe un risque que, sans cette recherche, des éléments de preuve soient perdus.

En cas d'extrême urgence, le juge d'instruction peut ordonner verbalement l'extension de la recherche visée à l'alinéa 1er. Cet ordre est confirmé par écrit dans les meilleurs délais, avec mention du flagrant délit ou des motifs de l'extrême urgence.";

5° l'article est complété par les paragraphes 5, 6, 7 et 8 rédigés comme suit:

"§ 5. En vue de permettre les mesures visée à cet article, le procureur du Roi ou le juge d'instruction peut également, sans le consentement du propriétaire ou de son ayant droit, ou de l'utilisateur, ordonner, à tout moment:

— la suppression temporaire de toute protection des systèmes informatiques concernés, le cas échéant à l'aide de moyens techniques, de faux signaux, de fausses clés ou de fausses qualités;

— l'installation de dispositifs techniques dans les systèmes informatiques concernés en vue du décryptage et du décodage de données stockées, traitées ou transmises par ce système.

Toutefois, seul le juge d'instruction peut ordonner cette suppression temporaire de protection ou cette installation de dispositifs techniques lorsque ceci est spécifiquement nécessaire pour l'application du paragraphe 3.

§ 6. Si des données stockées sont trouvées dans les systèmes informatiques concernés qui sont utiles pour les mêmes finalités que celles prévues pour la saisie, mais que la saisie du support n'est néanmoins pas souhaitable, ces données, de même que les données nécessaires pour les comprendre, sont copiées sur des supports qui appartiennent à l'autorité. En cas d'urgence ou pour des raisons techniques, il peut être fait usage de supports qui sont disponibles pour des personnes autorisées à utiliser le système informatique.

On utilise en outre les moyens techniques appropriés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à

om het informaticasysteem te gebruiken, te verhinderen en hun integriteit te waarborgen.

Wanneer de in het eerste lid vermelde maatregel niet mogelijk is om technische redenen of wegens de omvang van de gegevens, wendt de procureur des Konings de passende technische middelen aan om de toegang tot deze gegevens in het informaticasysteem, evenals tot de kopieën daarvan die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken, te verhinderen en hun integriteit te waarborgen.

Indien de gegevens het voorwerp van het misdrijf vormen of voortgekomen zijn uit het misdrijf en indien de gegevens strijdig zijn met de openbare orde of de goede zeden, of een gevaar opleveren voor de integriteit van informaticasystemen of gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen, wendt de procureur des Konings alle passende technische middelen aan om deze gegevens ontoegankelijk te maken of, na hiervan kopie te hebben genomen, te verwijderen.

Hij kan evenwel, behoudens in het geval bedoeld in het vorige lid, het verdere gebruik van het geheel of een deel van deze gegevens toestaan, wanneer dit geen gevaar voor de strafvordering oplevert.

In geval van uiterst dringende noodzakelijkheid en wanneer het kennelijk gaat om een strafbaar feit zoals bedoeld in de artikelen 137, § 3, 6°, 140*bis* of 383*bis*, § 1 van het Strafwetboek, kan de procureur des Konings mondeling bevelen dat alle passende technische middelen worden aangewend om de gegevens, die het voorwerp van het misdrijf vormen of voortgekomen zijn uit het misdrijf en die strijdig zijn met de openbare orde of de goede zeden, ontoegankelijk te maken. Dit bevel wordt zo spoedig mogelijk schriftelijk bevestigd, met vermelding van de redenen van de uiterst dringende noodzakelijkheid.

§ 7. Tenzij diens identiteit of woonplaats redelijkerwijze niet achterhaald kan worden, brengt de procureur des Konings of de onderzoeksrechter de verantwoordelijke van het informaticasysteem zo spoedig mogelijk op de hoogte van de zoeking in het informaticasysteem of van de uitbreiding ervan. Hij deelt hem in voorkomend geval een samenvatting mee van de gegevens die zijn gekopieerd, ontoegankelijk gemaakt of verwijderd.

§ 8. De procureur des Konings wendt de passende technische middelen aan om de integriteit en de vertrouwelijkheid van deze gegevens te waarborgen.

utiliser le système informatique, de même que pour garantir leur intégrité.

Lorsque la mesure prévue au § 2 n'est pas possible, pour des raisons techniques ou à cause du volume des données, le procureur du Roi utilise les moyens techniques appropriés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité.

Si les données forment l'objet de l'infraction ou ont été produites par l'infraction et si elles sont contraires à l'ordre public ou aux bonnes mœurs ou constituent un danger pour l'intégrité des systèmes informatiques ou pour des données stockées, traitées ou transmises par le biais de tels systèmes, le procureur du Roi utilise tous les moyens techniques appropriés pour rendre ces données inaccessibles ou, après en avoir pris copie, les retirer.

Il peut cependant, sauf dans le cas prévu à l'alinéa précédent, autoriser l'usage ultérieur de l'ensemble ou d'une partie de ces données, lorsque cela ne présente pas de danger pour l'exercice des poursuites.

En cas d'extrême urgence et s'il s'agit manifestement d'une infraction visée aux articles 137, § 3, 6°, 140*bis* ou 383*bis*, § 1er du Code pénal, le procureur du Roi peut ordonner verbalement que tous les moyens appropriés soient utilisés pour rendre inaccessibles les données qui forment l'objet de l'infraction ou ont été produites par l'infraction et qui sont contraires à l'ordre public ou aux bonnes mœurs. Cet ordre est confirmé par écrit dans les meilleurs délais, avec mention des motifs de l'extrême urgence.

§ 7. Sauf si son identité ou son adresse ne peuvent être raisonnablement retrouvées, le procureur du Roi ou le juge d'instruction informe dans les plus brefs délais, le responsable du système informatique de la recherche dans le système informatique ou de son extension. Il lui communique le cas échéant un résumé des données qui ont été copiées, rendues inaccessibles ou retirées.

§ 8. Le procureur du Roi utilise les moyens techniques appropriés pour garantir l'intégrité et la confidentialité de ces données.

Gepaste technische middelen worden aangewend voor de bewaring hiervan op de griffie.

Hetzelfde geldt, wanneer gegevens die worden opgeslagen, verwerkt of overgedragen in een informaticasysteem, samen met hun drager in beslag worden genomen, overeenkomstig de vorige artikelen.".

Artikel 3

In hetzelfde Wetboek wordt een artikel 39*ter* ingevoegd, luidende:

"Art. 39*ter*. § 1. Bij het opsporen van de misdaden en de wanbedrijven en onverminderd de bevoegdheden bedoeld in de artikelen 39*bis*, 46*bis* en 88*bis* van het Wetboek van strafvordering en de artikelen XII.17, XII.18, XII.19 en XII.20 van het Wetboek van Economisch Recht, kan iedere officier van gerechtelijke politie, wanneer er redenen bestaan om aan te nemen dat gegevens die opgeslagen, verwerkt of overgedragen worden door middel van een informaticasysteem bijzonder kwetsbaar zijn voor verlies of voor wijziging, bij een gemotiveerde en schriftelijke beslissing aan een of meerdere natuurlijke personen of rechtspersonen bevelen de gegevens die in hun bezit zijn of waarover zij controle hebben te bewaren.

De gemotiveerde en schriftelijke beslissing vermeldt:

— de naam en hoedanigheid van de officier van gerechtelijke politie die om de bewaring verzoekt;

— het strafbare feit waarop het verzoek betrekking heeft;

— de gegevens die bewaard moeten worden;

— de duur van bewaring van de gegevens, die niet langer mag zijn dan negentig dagen. Deze termijn kan schriftelijk worden verlengd.

In spoedeisende gevallen kan de opdracht tot bewaring mondeling worden gegeven. De opdracht moet zo spoedig mogelijk worden bevestigd in de vorm bepaald in het vorige lid.

§ 2. De natuurlijke personen of rechtspersonen bedoeld in § 1, zorgen ervoor dat de integriteit van de gegevens gewaarborgd is en dat de gegevens op een veilige manier bewaard worden.

§ 3. Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn

Des moyens techniques appropriés sont utilisés pour leur conservation au greffe.

La même règle s'applique, lorsque des données qui sont stockées, traitées ou transmises dans un système informatique sont saisies avec leur support, conformément aux articles précédents.".

Article 3

Dans le même Code, il est inséré un article 39*ter* rédigé comme suit:

"Art. 39*ter*. § 1er. Lors de la recherche de crimes et délits et sans préjudice des compétences visées aux articles 39*bis*, 46*bis* et 88*bis* du Code d'instruction criminelle et aux articles XII.17, XII.18, XII.19 et XII.20 du Code de droit économique, tout officier de police judiciaire peut, s'il existe des raisons de croire que des données stockées, traitées ou transmises par un système informatique au moyen d'un système informatique sont particulièrement susceptibles de perte ou de modification, ordonner, par une décision écrite motivée, à une ou plusieurs personnes physiques ou personnes morales de conserver les données qui sont en leur possession ou sous leur contrôle.

La décision écrite motivée mentionne:

— les nom et qualité de l'officier de police judiciaire commis pour l'exécution de la mesure;

— l'infraction qui fait l'objet de la recherche;

— les données qui doivent être conservées;

— la durée de conservation des données, qui ne peut excéder nonante jours. Ce délai peut être prolongé par écrit.

En cas d'urgence, la conservation peut être ordonnée verbalement. Elle doit être confirmée dans les plus brefs délais dans la forme prévue à l'alinéa précédent.

§ 2. Les personnes physiques ou personnes morales visées au § 1er veillent à ce que l'intégrité des données soit garantie et à ce que les données soient conservées de manière sécurisée.

§ 3. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours,

medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

Iedere persoon die weigert mee te werken, of die de bewaarde gegevens doet verdwijnen, vernietigt of wijzigt, wordt gestraft met een gevangenisstraf van zes maanden tot een jaar en met een geldboete van 26 tot 20 000 euro of met één van die straffen alleen.".

Artikel 4

In hetzelfde Wetboek wordt een artikel 39*quater* ingevoegd, luidende:

"Art. 39*quater*. § 1. Onverminderd de mogelijkheden tot rechtstreekse samenwerking met buitenlandse operatoren van elektronische communicatienetwerken en verstrekkers van elektronische communicatiediensten, kan de procureur des Konings, via de door de Koning aangewezen politiedienst, aan een buitenlandse bevoegde autoriteit verzoeken de snelle bewaring te bevelen of op andere wijze op te leggen van gegevens die opgeslagen, verwerkt of overgedragen worden door middel van een informaticasysteem dat zich bevindt op het grondgebied van die bevoegde autoriteit en ten aanzien waarvan een Belgische bevoegde gerechtelijke autoriteit voornemens is een verzoek om rechtshulp in te dienen.

Het verzoek om bewaring is schriftelijk en vermeldt:

— de naam en hoedanigheid van de autoriteit die om de bewaring verzoekt;

— het strafbare feit waarop het verzoek betrekking heeft en een korte uiteenzetting van de daarop betrekking hebbende feiten;

— de gegevens die bewaard moeten worden en het verband met het strafbare feit;

— alle beschikbare informatie met betrekking tot de bewaarder van de gegevens of de locatie van het informaticasysteem;

— de noodzaak van de bewaring;

— het feit dat een verzoek om rechtshulp ingediend zal worden met betrekking tot de bewaarde gegevens;

est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

Toute personne qui refuse de coopérer, ou qui fait disparaître, détruit ou modifie les données conservées, sera punie d'un emprisonnement de six mois à un an ou d'une amende de 26 euros à 20 000 euros ou d'une de ces peines seulement."

Article 4

Dans le même Code, il est inséré un article 39*quater* rédigé comme suit:

"Art. 39*quater*. § 1er. Sans préjudice des possibilités de collaboration directe avec des opérateurs de services de communications électroniques et des fournisseurs de services de communications électroniques étrangers, le procureur du Roi peut, par l'intermédiaire du service de police désigné par le Roi, demander à une autorité compétente étrangère d'ordonner ou d'imposer d'une autre façon la conservation rapide de données stockées, traitées ou transmises par un système informatique qui se trouvent sur le territoire de cette autorité compétente et au sujet desquelles une autorité judiciaire belge compétente a l'intention de soumettre une demande d'entraide judiciaire.

La demande de conservation est formulée par écrit et mentionne:

— les nom et qualité de l'autorité qui demande la conservation;

— l'infraction qui fait l'objet de la demande et un exposé succinct des faits qui y ont trait;

— les données à conserver et le lien avec l'infraction;

— toutes les informations disponibles concernant le dépositaire des données ou la localisation du système informatique;

— la nécessité de la conservation;

— le fait qu'une demande d'entraide judiciaire concernant les données conservées sera soumise;

— in voorkomend geval, het feit dat de gegevens die bewaard moeten worden verwijzen naar een andere staat dan de staat van de bevoegde buitenlandse autoriteit.

§ 2. Indien een internationaal rechtsinstrument tussen België en een andere Staat hierin voorziet, kan een bevoegde autoriteit van die Staat aan de door de Koning aangewezen politiedienst verzoeken de snelle bewaring te bevelen of op andere wijze op te leggen van gegevens die zich bevinden op het Belgische grondgebied en ten aanzien waarvan deze buitenlandse autoriteit voornemens is een verzoek om rechtshulp in te dienen.

Het verzoek om bewaring is schriftelijk en vermeldt:

— de naam en hoedanigheid van de autoriteit die om de bewaring verzoekt;

— het strafbare feit waarop het verzoek betrekking heeft en een korte uiteenzetting van de daarop betrekking hebbende feiten;

— de gegevens die bewaard moeten worden en het verband met het strafbare feit;

— alle beschikbare informatie met betrekking tot de bewaarder van de gegevens of de locatie van het informaticasysteem;

— de noodzaak van de bewaring, en

— het feit dat een verzoek om rechtshulp ingediend zal worden met betrekking tot de bewaarde gegevens;

— in voorkomend geval, het feit dat de gegevens die bewaard moeten worden verwijzen naar een andere staat dan de staat van de bevoegde buitenlandse autoriteit.

Na ontvangst van het verzoek bedoeld in het vorige lid, brengt de in het eerste lid bedoelde politiedienst de bevoegde procureur des Konings of onderzoeksrechter daarvan op de hoogte, en neemt zij alle passende maatregelen om onverwijld over te gaan tot de snelle bewaring van de nader omschreven gegevens, overeenkomstig artikel 39*ter*.

Onverminderd de internationale rechtsinstrumenten met betrekking tot rechtshulp waardoor België gebonden is en die ertoe strekken deze samenwerking te bevorderen, kan een verzoek om bewaring door de bevoegde procureur des Konings of onderzoeksrechter alleen worden geweigerd indien:

— le cas échéant, le fait que les données qui doivent être conservées renvoient à un autre État que l'État de l'autorité étrangère compétente.

§ 2. Lorsqu'une telle possibilité est prévue dans un instrument de droit international liant la Belgique et un autre État, une autorité compétente de cet État peut demander au service de police désigné par le Roi d'ordonner ou d'imposer d'une autre manière la conservation rapide de données stockées, traitées ou transmises par un système informatique qui se trouvent sur le territoire belge et au sujet desquelles cette autorité judiciaire étrangère a l'intention de soumettre une demande d'entraide judiciaire.

La demande de conservation est formulée par écrit et mentionne:

— les nom et qualité de l'autorité qui demande la conservation;

— l'infraction qui fait l'objet de la demande et un exposé succinct des faits qui y ont trait;

— les données à conserver et le lien avec l'infraction;

— toutes les informations disponibles concernant le dépositaire des données ou la localisation du système informatique;

— la nécessité de la conservation, et

— le fait qu'une demande d'entraide judiciaire concernant les données conservées sera soumise;

— le cas échéant, le fait que les données qui doivent être conservées renvoient à un autre État que l'État de l'autorité étrangère compétente.

Après réception de la demande visée à l'alinéa précédent, le service de police visé à l'alinéa 1er en informe le procureur du Roi ou le juge d'instruction compétent et prend toutes les mesures appropriées pour procéder sans délai à la conservation rapide des données définies conformément à l'article 39*ter*.

Sans préjudice des instruments de droit international liant la Belgique en matière d'entraide judiciaire et tendant à promouvoir celle-ci, une demande de conservation peut être rejetée à tout moment par le procureur du Roi ou le juge d'instruction compétent:

— het verzoek betrekking heeft op een misdrijf dat door België wordt beschouwd als politiek misdrijf of als een met een politiek misdrijf samenhangend feit, of

— de uitvoering van het verzoek zou kunnen leiden tot aantasting van de soevereiniteit, veiligheid, openbare orde of andere wezenlijke belangen van België.

Wanneer de in het eerste lid bedoelde politiedienst van mening is dat de gewone bewaring de toekomstige beschikbaarheid van de gegevens niet waarborgt of de vertrouwelijkheid van het onderzoek van de bevoegde buitenlandse autoriteit in gevaar brengt of dit anderszins schaadt, brengt zij de bevoegde buitenlandse autoriteit hiervan onverwijld op de hoogte, die vervolgens bepaalt of het verzoek niettemin moet worden uitgevoerd.

Een bewaring verricht in antwoord op het in het eerste lid bedoelde verzoek is geldig voor een periode van ten minste 60 dagen, teneinde de bevoegde buitenlandse autoriteit de mogelijkheid te bieden een verzoek om rechtshulp in te dienen. Na de ontvangst van een dergelijk verzoek blijven de gegevens bewaard in afwachting van een beslissing inzake het verzoek.

Indien de gegevens die opgeslagen, verwerkt of overgedragen worden door middel van een informaticasysteem verwijzen naar een andere staat dan de staat van de verzoekende bevoegde buitenlandse autoriteit, brengt de in het eerste lid bedoelde politiedienst de bevoegde procureur des Konings of onderzoeksrechter daarvan op de hoogte. Deze gaat zo snel mogelijk over tot de onthulling aan de bevoegde buitenlandse autoriteit van een hoeveelheid identificatiegegevens of oproepgegevens voldoende om te achterhalen wie die operator van het elektronische communicatienetwerk of de verstrekker van de elektronische communicatiedienst is en langs welke weg de communicatie was verzonden.”.

Artikel 5

In artikel 46*bis* van hetzelfde Wetboek, ingevoegd bij wet van 10 juni 1998 en gewijzigd bij de wetten van 27 december 2004, 23 januari 2007 en … (dataretentiewet) worden de volgende wijzigingen aangebracht:

1° paragraaf 1 wordt vervangen als volgt:

“§ 1. Bij het opsporen van de misdaden en wanbedrijven kan de procureur des Konings bij een gemotiveerde en schriftelijke beslissing overgaan of doen overgaan op basis van ieder gegeven in zijn bezit of door middel van een toegang tot de klantenbestanden van de actoren bedoeld in het tweede lid, eerste en tweede streepje, tot:

— si la demande concerne une infraction considérée par la Belgique comme une infraction politique ou un fait connexe à une infraction politique, ou

— si l’exécution de la demande est de nature à porter atteinte à la souveraineté, à la sécurité, à l’ordre public ou à d’autres intérêts essentiels de la Belgique.

Si le service de police visé à l’alinéa 1er estime que la conservation simple ne suffira pas à garantir la disponibilité future des données, ou compromettra la confidentialité de l’enquête de l’autorité étrangère compétente ou nuira d’une autre façon à celle-ci, il en informe sans délai l’autorité étrangère compétente, qui décide alors s’il convient néanmoins d’exécuter la demande.

Une conservation effectuée en réponse à la demande visée à l’alinéa 1er est valable pour une période d’au moins 60 jours afin d’offrir à l’autorité étrangère compétente la possibilité de soumettre une demande d’entraide judiciaire. Après réception d’une telle demande, les données restent conservées dans l’attente d’une décision concernant la demande.

Si les données qui sont stockées, traitées ou transmises par un système informatique renvoient à un autre État que l’État de l’autorité étrangère compétente requérante, le service de police visé à l’alinéa 1er en informe le procureur du Roi ou le juge d’instruction compétent. Celui-ci divulgue, dans les meilleurs délais, à l’autorité étrangère compétente une quantité de données d’identification ou d’appel suffisante pour retrouver qui est l’opérateur du réseau de communications électroniques ou le fournisseur du service de communications électroniques et par quelle voie la communication a été envoyée.”.

Article 5

A l’article 46*bis* du même Code, inséré par la loi du 10 juin 1998 et modifié par les lois du 27 décembre 2004, 23 janvier 2007 et … (loi dataretention) les modifications suivantes sont apportées:

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

“§ 1er. En recherchant les crimes et les délits, le procureur du Roi peut, par une décision motivée et écrite, procéder ou faire procéder sur la base de toutes données détenues par lui, ou au moyen d’un accès aux fichiers des clients des acteurs visés à l’alinéa 2, 1er et 2e tirets, à

1° de identificatie van de abonnee of de gewoonlijke gebruiker van een dienst zoals bedoeld in het tweede lid, tweede streepje, of van het gebruikte elektronische communicatiemiddel;

2° de identificatie van de diensten zoals bedoeld in het tweede lid, tweede streepje, waarop een bepaald persoon geabonneerd is of die door een bepaald persoon gewoonlijk gebruikt worden.

Hiertoe kan hij zo nodig, rechtstreeks of via de door de Koning aangewezen politiedienst, de medewerking vorderen van:

— de operator van een elektronisch communicatienetwerk; en

— iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.

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 de procureur des Konings de maatregel mondeling bevelen. De beslissing wordt zo spoedig mogelijk schriftelijk bevestigd.

Voor strafbare feiten die geen correctionele hoofdgevangenisstraf van een 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.";

2° in paragraaf 2 wordt het eerste lid vervangen als volgt:

"De actoren bedoeld in § 1, tweede lid, eerste en tweede streepje, van wie gevorderd wordt de in paragraaf 1 bedoelde gegevens mee te delen, verstrekken de procureur des Konings of de officier van gerechtelijke politie de gegevens die werden opgevraagd in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, volgens de modaliteiten vastgesteld door de Koning, op het voorstel van de minister van Justitie en de minister bevoegd voor Telecommunicatie.";

1° l'identification de l'abonné ou de l'utilisateur habituel d'un service visé à l'alinéa 2, deuxième tiret, ou bien du moyen de communication électronique utilisé;

2° l'identification des services visés à l'alinéa 2, deuxième tiret, auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée.

Si nécessaire, il peut pour ce faire requérir, directement ou par l'intermédiaire d'un service de police désigné par le Roi, la collaboration:

— de l'opérateur d'un réseau de communications électroniques;

— de toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.

La 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, le procureur du Roi peut ordonner verbalement cette mesure. La décision est confirmée par écrit dans les plus brefs délais

Pour des infractions qui qui ne sont pas de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde, le procureur du Roi ne peut requérir les données visées à l'alinéa 1er que pour une période de six mois préalable à sa décision.";

2° dans le paragraphe 2, le premier alinéa est remplacé par ce qui suit:

"Les acteurs visés au § 1er, alinéa 2, 1er et 2e tirets, requis de communiquer les données visées au § 1er fournissent au procureur du Roi ou à l'officier de police judiciaire les données qui ont été demandées en temps réel ou, le cas échéant, au moment précisé dans la réquisition, selon les modalités fixées par le Roi, sur la proposition du ministre de la Justice et du ministre compétent pour les Télécommunications.";

3° in paragraaf 2 wordt het laatste lid vervangen als volgt:

"Iedere persoon die de gegevens weigert mee te delen of niet meedeelt in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, wordt gestraft met geldboete van zesentwintig euro tot tienduizend euro.".

Artikel 6

In artikel 46*quinquies* van hetzelfde Wetboek, ingevoegd bij wet van 27 december 2005, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1 worden de woorden "en gesloten voorwerpen die zich op deze plaats bevinden te openen" ingevoegd tussen de woorden "een private plaats te betreden" en de woorden ", wanneer er ernstige aanwijzingen zijn";

2° in paragraaf 2 worden de woorden "betreden van de private plaats zoals bedoeld in § 1" vervangen door de woorden "betreden van de private plaats zoals bedoeld in § 1, en het openen van gesloten voorwerpen die zich op deze plaats bevinden,";

3° in paragraaf 2 wordt de bepaling onder 3°, aangevuld met de woorden ", te herstellen of terug te nemen;";

4° paragraaf 2 wordt aangevuld met de bepaling onder 4°, luidende:

"4° de overeenkomstig § 5 meegenomen voorwerpen terug te plaatsen.";

5° het artikel wordt aangevuld met de paragrafen 5, 6 en 7, luidende: "§ 5. Indien het onderzoek van een in § 1 bedoeld voorwerp niet ter plaatse kan gebeuren en indien de informatie niet op een andere manier kan worden verkregen, is het de politiedienst toegestaan dit voorwerp mee te nemen voor een strikt beperkte duur. Het bewuste voorwerp wordt zo spoedig mogelijk teruggeplaatst, tenzij dit het goede verloop van het onderzoek in de weg staat.

§ 6. In het kader van de maatregel bedoeld in § 1, is het binnendringen in een informaticasysteem enkel mogelijk met het oog op de doeleinden bedoeld in § 2, 3°.

§ 7. De officier van gerechtelijke politie die de leiding heeft over de uitvoering van de maatregel bedoeld in § 1 of in artikel 89*ter*, § 1, stelt van het verloop van de

3° dans le paragraphe 2, le dernier alinéa est remplacé par ce qui suit:

"Toute personne qui refuse de communiquer les données ou qui ne les communique pas en temps réel ou, le cas échéant, au moment précisé dans la réquisition est punie d'une amende de vingt-six euros à dix mille euros.".

Article 6

A l'article 46*quinquies* du même Code, inséré par la loi du 27 décembre 2005, les modifications suivantes sont apportées:

1° dans le paragraphe premier, les mots "et à ouvrir les objets fermés se trouvant dans ce lieu," sont insérés entre les mots "à tout moment dans un lieu privé" et "à l'insu du propriétaire";

2° dans le paragraphe 2, les mots "pénétration du lieu privé visé au § 1er," sont remplacés par les mots "pénétration du lieu privé visé au § 1er, et l'ouverture des objets fermés se trouvant sur ce lieu,";

3° dans le paragraphe 2, le 3° est remplacé par ce qui suit: "3° de réparer ou de retirer dans le cadre d'une observation un moyen technique visé à l'article 47*sexies*, § 1er, alinéa 3;";

4° le paragraphe 2 est complété par le 4° rédigé comme suit:

"4º de replacer les objets emportés conformément au § 5.";

5° l'article est complété par les paragraphes 5,6 et 7 rédigés comme suit: "§ 5. Si l'examen d'un objet visé au § 1er ne peut se faire sur place et si l'information ne peut être obtenue d'une autre manière, le service de police est autorisé à emporter cet objet pour une durée strictement limitée. L'objet en question est remis en place dans les plus brefs délais, à moins que cela n'entrave le bon déroulement de l'enquête.

§ 6. Dans le cadre de la mesure visée au § 1er, la pénétration dans un système informatique n'est possible qu'aux fins visées au § 2, 3°.

§ 7. L'officier de police judiciaire qui dirige l'exécution de la mesure visé au § 1er ou à l'article 89*ter*, § 1er, rédige un procès-verbal du cours de la mesure. Lorsque des

maatregel een proces-verbaal op. Wanneer tijdens de uitvoering van de maatregel gesloten voorwerpen geopend werden of toepassing gemaakt werd van § 5, wordt daarvan melding gemaakt in het proces-verbaal. Het proces-verbaal wordt uiterlijk na het beëindigen van de maatregel bij het strafdossier gevoegd.".

Artikel 7

In hetzelfde Wetboek wordt een artikel 46*sexies* ingevoegd, luidende:

"Art. 46*sexies*. § 1. Bij het opsporen van de misdaden en de wanbedrijven, wanneer het onderzoek zulks vereist en de overige middelen van onderzoek niet lijken te volstaan om de waarheid aan de dag te brengen, kan de procureur des Konings de politiediensten bedoeld in het tweede lid machtigen om op het internet, desgevallend onder een fictieve identiteit, contact te onderhouden met een of meerdere personen waarvan er ernstige aanwijzingen zijn dat zij strafbare feiten die een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben, plegen of zouden plegen.

De Koning bepaalt de voorwaarden, onder meer voor wat de opleiding betreft, en de modaliteiten voor de aanwijzing van de politiediensten die bevoegd zijn om de maatregel, bedoeld in dit artikel, ten uitvoer te leggen.

In uitzonderlijke omstandigheden en mits uitdrukkelijke machtiging van de procureur des Konings, kan de in het eerste lid bedoelde politieambtenaar bij een welbepaalde operatie kortstondig een beroep doen op de deskundigheid van een persoon die niet tot de politiediensten behoort, indien dit strikt noodzakelijk voorkomt voor het welslagen van zijn opdracht.

Dit artikel is niet van toepassing op de persoonlijke interactie op het internet van politieambtenaren, bij de uitvoering van hun opdrachten van gerechtelijke politie, met een of meerdere personen, die enkel een gerichte verificatie of een arrestatie tot direct doel heeft, en dit zonder gebruik te maken van een geloofwaardige fictieve identiteit.

§ 2. De maatregel bedoeld in § 1 wordt door de procureur des Konings bevolen met een voorafgaandelijke en met redenen omklede schriftelijke machtiging. Deze machtiging is geldig voor een termijn van drie maanden, onverminderd hernieuwing.

objets fermés sont ouverts ou qu'il est fait application du § 5 durant l'exécution de la mesure, il en est fait mention dans le procès-verbal. Le procès-verbal est joint au dossier répressif au plus tard après qu'il a été mis fin à la mesure.".

Article 7

Dans le même Code, il est inséré un article 46*sexies* rédigé comme suit:

"Art. 46*sexies*. § 1er. Dans la recherche des crimes et délits, si les nécessités de l'enquête l'exigent et que les autres moyens d'investigation ne semblent pas suffire à la manifestation de la vérité, le procureur du Roi peut autoriser les services de police visés à l'alinéa 2 à entretenir, le cas échéant sous une identité fictive, des contacts avec une ou plusieurs personnes concernant lesquelles il existe des indices sérieux qu'elles commettent ou commettraient des infractions pouvant donner lieu à un emprisonnement correctionnel principal d'un an ou à une peine plus lourde.

Le Roi détermine les conditions, y compris pour ce qui concerne la formation, et les modalités de désignation des services de police habilités à exécuter la mesure visée au présent article.

Dans des circonstances exceptionnelles et moyennant l'autorisation expresse du procureur du Roi, le fonctionnaire de police visé à l'alinéa 1er peut, dans le cadre d'une opération déterminée, momentanément recourir à l'expertise d'une personne qui ne fait pas partie des services de police si cela s'avère strictement nécessaire à la réussite de sa mission.

Le présent article ne s'applique pas à l'interaction personnelle de fonctionnaires de police, dans l'exercice de leurs missions de police judiciaire, avec une ou plusieurs personnes sur Internet, qui n'a pour finalité directe qu'une vérification ciblée ou une arrestation, et ceci sans utiliser d'identité fictive crédible.

§ 2. La mission visée au § 1er est ordonnée par le procureur du Roi par une autorisation écrite et motivée préalable. Cette autorisation est valable pour une période de trois mois, sous réserve de renouvellement.

In spoedeisende gevallen kan de machtiging mondeling worden verstrekt. De machtiging moet zo spoedig mogelijk worden bevestigd in de vorm bepaald in het eerste lid.

§ 3. Blijven vrij van straf de politieambtenaren die, in het kader van hun opdracht en met het oog op het welslagen ervan of ter verzekering van hun eigen veiligheid of deze van andere bij de maatregel betrokken personen, strikt noodzakelijke strafbare feiten plegen, mits uitdrukkelijk akkoord van de procureur des Konings.

Die strafbare feiten mogen niet ernstiger zijn dan die waarvoor de maatregel wordt aangewend en moeten noodzakelijkerwijze evenredig zijn met het nagestreefde doel.

Het eerste en het tweede lid zijn eveneens van toepassing op de personen die aan de uitvoering van deze opdracht noodzakelijke en rechtstreekse hulp of bijstand hebben verleend en op de personen, bedoeld in § 1, derde lid.

Blijft vrij van straf de magistraat die, met inachtneming van dit wetboek, machtiging verleent aan een politieambtenaar en aan de personen bedoeld in het derde lid tot het plegen van strafbare feiten in het kader van de uitvoering van de maatregel.

De politieambtenaren melden schriftelijk en vóór de uitvoering van de maatregel aan de procureur des Konings, de misdrijven die zij of de personen bedoeld in het derde lid, voornemens zijn te plegen.

Indien deze voorafgaande kennisgeving niet kon gebeuren, stellen de politieambtenaren de procureur des Konings onverwijld in kennis van de misdrijven die zij of de personen bedoeld in het derde lid, hebben gepleegd en bevestigen dit nadien schriftelijk.

De procureur des Konings vermeldt in een afzonderlijke en schriftelijke beslissing de misdrijven die door de politiediensten en de personen bedoeld in het derde lid in het kader van deze door hem bevolen maatregel kunnen worden gepleegd. Deze beslissing wordt in een afzonderlijk en vertrouwelijk dossier bewaard. Hij heeft als enige toegang tot dit dossier, onverminderd het in artikel 56*bis*, respectievelijk de artikelen 235*ter*, § 3 en 235*quater*, § 3 bedoelde inzagerecht van de onderzoeksrechter en de kamer van inbeschuldigingstelling. De inhoud van dit dossier valt onder het beroepsgeheim.

§ 4. De met het onderzoek belaste officier van gerechtelijke politie stelt proces-verbaal op van de verschillende fasen in de uitvoering van deze maatregel, met inbegrip

En cas d'urgence, l'autorisation peut être donnée verbalement. Elle doit être confirmée dans les plus brefs délais dans la forme prévue à l'alinéa précédent.

§ 3. Sont exemptés de peine, les fonctionnaires de police qui, dans le cadre de leur mission et en vue de la réussite de celle-ci ou afin de garantir leur propre sécurité ou celle d'autres personnes, commettent des infractions strictement nécessaires, ce avec l'accord exprès du procureur du Roi.

Ces infractions ne peuvent être plus graves que celles pour laquelle la mesure est utilisée et doivent nécessairement être proportionnelles à l'objectif visé.

Les alinéas 1er et 2 sont également d'application aux personnes qui ont fourni directement une aide ou une assistance nécessaire à l'exécution de cette mission ainsi qu'aux personnes visées au § 1er, alinéa 3.

Sont exemptés de peine, les magistrats qui autorisent, dans le respect du présent code, un fonctionnaire de police et la personne visée à l'alinéa 3 à commettre des infractions dans le cadre de l'exécution de la mesure.

Les fonctionnaires de police communiquent, par écrit et préalablement à l'exécution de la mesure, au procureur du Roi les infractions qu'eux-mêmes ou les personnes visées à l'alinéa 3 ont l'intention de commettre.

Si cette notification préalable n'a pas pu avoir lieu, les fonctionnaires de police informent sans délai le procureur du Roi des infractions qu'eux-mêmes ou les personnes visées à l'alinéa 3 ont commises et en donnent ensuite confirmation par écrit.

Le procureur du Roi énonce dans une décision écrite séparée les infractions pouvant être commises par les services de police et les personnes visées à l'alinéa 3 dans le cadre de la mesure ordonnée par lui. Cette décision est conservée dans un dossier séparé et confidentiel. Il est le seul à avoir accès à ce dossier, sans préjudice du droit de consultation du juge d'instruction et de la chambre des mises en accusation visé respectivement à l'article 56*bis* et aux articles 235*ter*, § 3, et 235*quater*, § 3. Le contenu de ce dossier est couvert par le secret professionnel.

§ 4. L'officier de police judiciaire chargé de l'enquête rédige le procès-verbal des différentes phases de l'exécution de cette mesure, y compris les contacts

van de relevante contacten. Deze processen-verbaal worden uiterlijk na het beëindigen van de maatregel bij het dossier gevoegd.

De contacten bedoeld in § 1 worden met de passende technische middelen geregistreerd en uiterlijk na het beëindigen van de maatregel bij het dossier gevoegd of ter griffie, al dan niet in digitale vorm, neergelegd.

§ 5. De procureur des Konings staat in voor de tenuitvoerlegging van de machtigingen tot de maatregel bedoeld in § 1, eerste lid, die zijn verleend door de onderzoeksrechter in het kader van een gerechtelijk onderzoek overeenkomstig artikel 56*bis*.

De procureur des Konings vermeldt op dat ogenblik in een afzonderlijke en schriftelijke beslissing de misdrijven die door de politiediensten en de personen bedoeld § 3, derde lid, in het kader van de door de onderzoeksrechter bevolen maatregel kunnen worden gepleegd. Deze beslissing wordt in het dossier bedoeld in § 3, zevende lid, bewaard.".

pertinents. Ces procès-verbaux sont joints au dossier au plus tard après la fin de la mesure.

Les contacts visés au § 1er sont enregistrés avec les moyens techniques appropriés et joints au dossier ou déposés au greffe, sous forme numérique ou non, au plus tard après la fin de la mesure.

§ 5. Le procureur du Roi est chargé de l'exécution des autorisations de la mesure visée au § 1er, alinéa 1er, accordées par le juge d'instruction dans le cadre d'une instruction, conformément à l'article 56*bis*.

Le procureur du Roi énonce à ce moment dans une décision écrite séparée les infractions pouvant être commises par les services de police et les personnes visées au § 3, alinéa 3, dans le cadre de la mesure ordonnée par le juge d'instruction. Cette décision est conservée dans le dossier visé au § 3, alinéa 7.".

Artikel 8

In artikel 47*sexies* van hetzelfde Wetboek, ingevoegd bij wet van 6 januari 2003 en gewijzigd bij wet van 27 december 2005, worden de volgende wijzigingen aangebracht:

1° de bepaling onder paragraaf 3, 1°, wordt vervangen als volgt:

"1° de ernstige aanwijzingen van het strafbaar feit die de observatie wettigen, of, indien de observatie zich situeert in het proactieve onderzoek zoals omschreven in artikel 28*bis*, § 2, het redelijk vermoeden van te plegen of reeds gepleegde maar nog niet aan het licht gebrachte strafbare feiten, en de bijzondere aanwijzingen met betrekking tot de elementen omschreven in deze laatste bepaling, die de observatie wettigen;";

2° in de bepaling onder § 3, 5°, worden de woorden "één maand" vervangen door de woorden "drie maanden";

3° in paragraaf 5 worden de woorden "het eerste lid" vervangen door de woorden "§ 3".

Article 8

A l'article 47*sexies*, § 3 du même Code, inséré par la loi du 6 janvier 2003 et modifié par la loi du 27 décembre 2005, les modifications suivantes sont apportées:

1° paragraphe 3, 1°, est remplacé par ce qui suit:

"1° les indices sérieux de l'infraction qui justifient l'observation ou, si l'observation s'inscrit dans le cadre de l'enquête proactive définie à l'article 28*bis*, § 2, la suspicion raisonnable que des faits punissables vont être commis ou ont été commis mais ne sont pas encore connus, et les indices particuliers relatifs aux éléments décrits dans cette dernière disposition, qui justifient l'observation;";

2° au § 3, 5°, les mots "un mois" sont remplacés par les mots "trois mois".

3° au paragraphe 5, les mots "à l'alinéa 1er" sont remplacés par les mots "au § 3".

Artikel 9

In artikel 47*octies* van hetzelfde Wetboek, ingevoegd bij de wet van 6 januari 2003, gewijzigd door de wet van

Article 9

Dans l'article 47*octies* du même Code, inséré par la loi de 6 janvier 2003, modifié par la loi de

27 december 2005 en de wet van 29 december 2010, worden de volgende wijzigingen aangebracht:

1° de bepaling onder § 3, 1°, wordt aangevuld met de woorden “of, indien de infiltratie zich situeert in het proactieve onderzoek zoals omschreven in artikel 28*bis*, § 2, het redelijk vermoeden van te plegen of reeds gepleegde maar nog niet aan het licht gebrachte strafbare feiten, en de bijzondere aanwijzingen met betrekking tot de elementen omschreven in deze laatste bepaling, die de infiltratie wettigen;”;

2° in paragraaf 5 worden de woorden “het eerste lid” vervangen door de woorden “§ 3”.

Artikel 10

In artikel 47*undecies* van hetzelfde Wetboek, ingevoerd bij de wet van 27 december 2005 en gedeeltelijk vernietigd bij arrest nr. 105/2007 van het Grondwettelijk Hof, wordt het laatste lid opgeheven.

Artikel 11

In artikel 56*bis* van hetzelfde Wetboek, ingevoegd bij de wet van 6 januari 2003 en gewijzigd bij wet van 27 december 2005, worden de volgende wijzigingen aangebracht:

1° in lid 1 worden de woorden “of een maatregel zoals bedoeld in artikel 46*sexies*” ingevoegd tussen de woorden “bijzondere opsporingsmethoden” en de woorden “beveelt ten uitvoer gelegd”;

2° lid 1 wordt aangevuld met de woorden: “, respectievelijk artikel 46*sexies*.”;

3° lid 4 wordt aangevuld met de volgende zin:

“Deze personen zijn tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.”.

Artikel 12

In artikel 88*bis* van hetzelfde Wetboek, ingevoegd bij de wet van 11 februari 1991 en gewijzigd bij de wetten van 30 juni 1994, 10 juni 1998, 8 juni 2008, 27 december 2012 en xxx (dataretentiewet) worden de volgende wijzigingen aangebracht:

1° paragraaf 1 wordt vervangen als volgt:

27 décembre 2005 et la loi de 29 décembre 2010, les modifications suivantes sont apportées:

1° le § 3, 1°, est complété par les mots “ou, si l’infiltration s’inscrit dans le cadre de l’enquête proactive définie à l’article 28*bis*, § 2, la suspicion raisonnable que des faits punissables vont être commis ou ont été commis mais ne sont pas encore connus, et les indices particuliers relatifs aux éléments décrits dans cette dernière disposition, qui justifient l’infiltration;”;

2° dans le paragraphe 5, les mots “à l’alinéa 1er” sont remplacés par les mots “au § 3”.

Article 10

Dans l’article 47*undecies* du même Code, inséré par la loi de 27 décembre 2005 et partiellement annulé par l’arrêt n° 105/2007 de la Cour constitutionnelle, le dernier alinéa est abrogé.

Article 11

A l’article 56*bis* du même code, inséré par la loi du 6 janvier 2003 et modifié par la loi du 27 décembre 2005, les modifications suivantes sont apportées:

1° dans l’alinéa 1 les mots “ou une mesure visée à l’article 46*sexies*” sont insérés entres les mots “de recherche” et les mots “sont exécutées”;

2° l’alinéa 1 est complété par les mots “et 46*sexies* respectivement.”;

3° l’alinéa 4 est complété par la phrase suivante:

“Ces personnes sont tenues au secret. Toute violation du secret est punie conformément à l’article 458 du Code pénal.”.

Article 12

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, 27 décembre 2012 et xxx (loi data retention), les modifications suivantes sont apportées:

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

"§ 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:

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.

Hiertoe kan hij zo nodig, rechtstreeks of via de door de Koning aangewezen politiedienst, de medewerking vorderen van:

— de operator van een elektronisch communicatienetwerk; en

— iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.

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 doet in een met redenen omkleed 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.

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 paragraaf 2.

"§ 1er. S'il existe des indices sérieux que les infractions sont de nature à entraîner un emprisonnement correctionnel principal d'un an ou 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:

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.

Si nécessaire, il peut pour ce faire requérir, directement ou par l'intermédiaire d'un service de police désigné par le Roi, la collaboration:

— de l'opérateur d'un réseau de communications électroniques; et

— de toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.

Dans les cas visés à l'alinéa 1er, pour chaque 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, 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 également 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 paragraphe 2.

In geval van ontdekking op heterdaad kan de procureur des Konings de maatregel bevelen voor de in artikel 90*ter*, §§ 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 347*bis*, 434 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 § 3*bis* 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 vierde en vijfde lid.";

2° aan paragraaf 3, lid 2, wordt een zin toegevoegd, luidende:

"Deze personen zijn tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.".

3° in paragraaf 4 wordt lid 1 vervangen als volgt:

"De actoren bedoeld in § 1, tweede lid, delen de gegevens waarom verzocht werd mee in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, volgens de modaliteiten vastgesteld door de Koning, op voorstel van de minister van Justitie en de minister bevoegd voor Telecommunicatie.";

4° in paragraaf 4 wordt het derde lid vervangen als volgt:

"Iedere persoon die zijn technische medewerking aan de vorderingen bedoeld in dit artikel weigert of niet verleent in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, 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 euro tot tienduizend euro.".

En cas de flagrant délit, le procureur du Roi peut ordonner la mesure pour les infractions visées à l'article 90*ter*, §§ 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 347*bis*, 434 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 § 3*bis* 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 4 et 5.";

2° paragraphe 3, alinéa 2, est complété par la phrase suivante:

"Ces personnes sont tenues au secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.".

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

"Les acteurs visés au § 1er, alinéa 2, communiquent les informations demandées en temps réel ou, le cas échéant, au moment précisé dans la réquisition, selon les modalités fixées par le Roi, sur la proposition du ministre de la Justice et du ministre compétent pour les Télécommunications.";

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

"Toute personne qui refuse de prêter son concours technique aux réquisitions visées au présent article, concours dont les modalités sont fixées par le Roi, sur la proposition du ministre de la Justice et du ministre compétent pour les Télécommunications, ou ne le prête pas en temps réel ou, le cas échéant, au moment précisé dans la réquisition, est punie d'une amende de vingt-six euros à dix mille euros.".

Artikel 13

Artikel 88*ter* van hetzelfde Wetboek, ingevoegd bij de wet van 28 november 2000 en gewijzigd bij de wet van 6 juni 2010, wordt opgeheven.

Artikel 14

In 88*quater* van hetzelfde Wetboek, ingevoegd bij wet van 28 november 2000 en gewijzigd bij de wet van 6 juni 2010, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1 wordt het woord "personen" vervangen door de woorden "aan eenieder" en worden de woorden "of de uitbreiding ervan zoals bedoeld in artikel 39*bis*" ingevoegd tussen de woorden "het voorwerp uitmaakt van de zoeking" en de woorden "of van diensten om gegevens die worden opgeslagen";

2° paragraaf 3 wordt vervangen als volgt:

"§ 3. Hij die de in §§ 1 en 2 gevorderde medewerking niet verleent of de zoeking in het informaticasysteem of de uitbreiding ervan hindert, wordt gestraft met gevangenisstraf van zes maanden tot drie jaar en met geldboete van zesentwintig euro tot twintigduizend euro of met een van die straffen alleen.

Wanneer de medewerking bedoeld in het eerste lid de uitvoering van een misdaad of een wanbedrijf kan verhinderen, of de gevolgen ervan kan beperken, en deze medewerking niet verleend wordt, zijn de straffen een gevangenisstraf van één tot vijf jaar en een geldboete van vijfhonderd tot vijftigduizend euro.".

Artikel 15

In artikel 89*ter* van hetzelfde Wetboek, ingevoegd bij de wet van 6 januari 2003 en gewijzigd bij de wet van 27 december 2005, wordt het eerste lid vervangen als volgt:

"In het kader van de uitvoering van de in artikel 46*quinquies* bepaalde maatregel, en onder de voorwaarden en met het oog op de doeleinden daar vermeld, kan alleen de onderzoeksrechter de politiedienst aangewezen door de Koning machtigen om:

— buiten medeweten van de eigenaar of van zijn rechthebbende, of van de bewoner, of zonder hun toestemming, te allen tijde een andere private plaats dan die

Article 13

L'article 88*ter* du même Code, inséré par la loi du 28 novembre 2000 et modifié par la loi du 6 juin 2010, est abrogé.

Article 14

A l'article 88*quater* du même Code, inséré par la loi du 28 novembre 2000 et modifié par la loi du 6 juin 2010, les modifications suivantes sont apportées:

1° dans le paragraphe 1er les mots "aux personnes" sont remplacés par les mots "à quiconque", et les mots "ou de son extension visée à l'article 39*bis*" sont insérés entre les mots "qui fait l'objet de la recherche" et les mots "ou des services qui permettent de protéger";

2 ° le paragraphe 3 est remplacé par ce qui suit:

"§ 3. Celui qui refuse de fournir la collaboration ordonnée aux §§ 1er et 2 ou qui fait obstacle à la recherche ou à son extension dans le système informatique, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à vingt mille euros ou d'une de ces peines seulement.

Si la collaboration visée à l'alinéa 1er peut empêcher la commission d'un crime ou d'un délit ou peut en limiter les effets et que cette collaboration n'est pas fournie, les peines sont un emprisonnement de un à cinq ans et une amende de cinq cents euros à cinquante mille euros.".

Article 15

A l'article 89*ter* du même Code, inséré par la loi du 6 janvier 2003 et modifié par la loi du 27 décembre 2005, l'alinéa 1er est remplacé par ce qui suit:

"Dans le cadre de l'exécution de la mesure prévue à l'article 46*quinquies*, et aux conditions ainsi qu'aux fins qu'il énonce, seul le juge d'instruction peut autoriser le service de police d'signer par le Roi à:

— pénétrer à tout moment dans un lieu privé autre que celui visé à l'article 46*quinquies*, § 1er, en ce compris ouvrir les objets fermés se trouvant dans ce lieu, à l'insu

welke bedoeld is artikel 46*quinquies*, § 1, te betreden, met inbegrip van het openen van gesloten voorwerpen die zich op deze plaats bevinden;

— buiten medeweten van de eigenaar, de bezitter of de gebruiker of zonder hun toestemming, zich toegang te verschaffen tot een informaticasysteem en het te doorzoeken, onverminderd de mogelijkheid voor de procureur des Konings om het binnendringen in een informaticasysteem te machtigen binnen de grenzen bepaald in artikel 46*quinquies*, § 6.".

Artikel 16

In het hetzelfde Wetboek wordt het opschrift van Boek 1, Hoofdstuk VI, Afdeling II, Onderafdeling II, paragraaf 6 vervangen als volgt:

"§ 6. Onderscheppen, kennisnemen, doorzoeken en opnemen van niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem of een deel ervan.".

Artikel 17

In artikel 90*ter* van hetzelfde Wetboek, ingevoerd bij de wet van 30 juni 1994 en laatstelijk gewijzigd bij de wet van 20 juli 2015, worden de volgende wijzigingen aangebracht:

1° paragraaf 1 wordt vervangen als volgt:

"§ 1. De onderzoeksrechter kan, onverminderd de toepassing van artikelen 39*bis*, 87, 88, 89*bis* en 90, met een heimelijk oogmerk, niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem of een deel ervan met technische hulpmiddelen onderscheppen, er kennis van nemen, doorzoeken en opnemen of de zoeking in een informaticasysteem of een deel ervan uitbreiden.

Deze maatregel kan enkel worden bevolen in uitzonderlijke gevallen, wanneer het onderzoek zulks vereist, indien er ernstige aanwijzingen bestaan dat het een strafbaar feit betreft bedoeld in een van de bepalingen opgesomd in § 2, en indien de overige middelen van onderzoek niet volstaan om de waarheid aan de dag te brengen.

Teneinde deze maatregel mogelijk te maken, kan de onderzoeksrechter bevelen om, te allen tijde, ook buiten medeweten of zonder de toestemming van hetzij de bewoner, hetzij de eigenaar of zijn rechthebbende, hetzij de gebruiker:

du propriétaire ou de son ayant droit, ou de l'occupant, ou sans le consentement de ceux-ci;

— s'introduire dans un système informatique et l'explorer, à l'insu du propriétaire, du détenteur ou de l'utilisateur ou sans leur consentement, sans préjudice de la possibilité pour le procureur du Roi d'autoriser l'introduction dans un système informatique dans les limites visées à l'article 46*quinquies*, § 6.".

Article 16

Dans le même Code, l'intitulé du Livre 1, Chapitre VI, Section II, Distinction II, paragraphe 6 est remplacé par ce qui suit:

"§ 6. Intercepter, prendre connaissance, explorer et enregistrer des communications non accessibles au public ou des données d'un système informatique ou d'une partie de celui-ci.".

Article 17

A l'article 90*ter* du même Code, inséré par la loi du 30 juin 1994 et modifié en dernier lieu par la loi du 20 juillet 2015, les modifications suivantes sont apportées:

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

"§ 1er. Sans préjudice de l'application des articles 39*bis*, 87, 88, 89*bis* et 90, le juge d'instruction peut, dans un but secret, intercepter, prendre connaissance, explorer et enregistrer, à l'aide de moyens techniques, des communications non accessibles au public ou des données d'un système informatique ou d'une partie de celui-ci, ou étendre une recherche dans un système informatique ou une partie de celui-ci.

Cette mesure ne peut être ordonnée que dans des cas exceptionnels, lorsque les nécessités de l'instruction l'exigent, s'il existe des indices sérieux que cela concerne une infraction visée par l'une des dispositions énumérées au § 2, et si les autres moyens d'investigation ne suffisent pas à la manifestation de la vérité.

En vue de permettre cette mesure, le juge d'instruction peut également, à l'insu ou sans le consentement de l'occupant, du propriétaire ou de son ayant droit, ou de l'utilisateur, ordonner, à tout moment:

— in een woning, in een private plaats of in een informaticasysteem binnen te dringen;

— elke beveiliging van de betrokken informaticasystemen tijdelijk op te heffen, desgevallend met behulp van technische hulpmiddelen, valse signalen, valse sleutels of valse hoedanigheden;

— technische middelen in de betrokken informaticasystemen aan te brengen teneinde de door dat systeem opgeslagen, verwerkte of doorgestuurde gegevens te ontcijferen en te decoderen.

De maatregel bedoeld in deze paragraaf kan alleen worden bevolen om de gegevens op te sporen die kunnen dienen om de waarheid aan de dag te brengen. Hij kan alleen worden bevolen ten aanzien van personen die op grond van precieze aanwijzingen ervan verdacht worden het strafbare feit te hebben gepleegd, ten aanzien van de communicatiemiddelen of informaticasystemen die geregeld worden gebruikt door een persoon op wie een verdenking rust of ten aanzien van de plaatsen waar deze vermoed wordt te vertoeven. De maatregel kan eveneens worden bevolen ten aanzien van personen van wie op grond van precieze feiten vermoed wordt dat zij geregeld in verbinding staan met een persoon op wie een verdenking rust.";

2° paragraaf 2 wordt vervangen als volgt:

"§ 2. De strafbare feiten die de maatregel bedoeld in § 1 kunnen wettigen zijn degene die bedoeld worden in:

1° de artikelen 101 tot en met 110 van het Strafwetboek;

2° De artikelen 136*bis*, 136*ter*, 136*quater*, 136*sexies* en 136*septies* van hetzelfde Wetboek en artikel 41 van de wet van 29 maart 2004 betreffende de samenwerking met het Internationaal Strafgerechtshof en de internationale straftribunalen;

3° Boek II, Titel Iter, van hetzelfde Wetboek;

4° artikel 147 van hetzelfde Wetboek;

5° de artikelen 160, 161, 162, 163, 168, 171, 173 en 176 van hetzelfde Wetboek;

6° de artikelen 180 en 186 van hetzelfde Wetboek;

7° artikel 210*bis* van hetzelfde Wetboek;

8° de artikelen 246, 247, 248, 249, en 250 van hetzelfde Wetboek;

9° artikel 259*bis* van hetzelfde Wetboek;

— la pénétration dans un domicile, un lieu privé ou un système informatique;

— la suppression temporaire de toute protection des systèmes informatiques concernés, le cas échéant à l'aide de moyens techniques, de faux signaux, de fausses clés ou de fausses qualités;

— l'installation de dispositifs techniques dans les systèmes informatiques concernés en vue du décryptage et du décodage de données stockées, traitées ou transmises par ce système.

La mesure visée dans ce paragraphe peut uniquement être ordonnée pour rechercher les données qui peuvent servir à la manifestation de la vérité. Elle ne peut être ordonnée qu'à l'égard soit de personnes soupçonnées, sur la base d'indices précis, d'avoir commis l'infraction, soit à l'égard des moyens de communication ou systèmes informatiques régulièrement utilisés par un suspect, soit à l'égard des lieux présumés fréquentés par celui-ci. Elle peut également être ordonnée à l'égard de personnes présumées, sur la base de faits précis, être en communication régulière avec un suspect.";

2° le paragraphe 2 est remplacé par ce qui suit:

"§ 2. Les infractions pouvant justifier la mesure visée au § 1er sont celles qui sont visées:

1° aux articles 101 à 110 du Code pénal;

2° aux articles 136*bis*, 136*ter*, 136*quater*, 136*sexies* et 136*septies* du même Code et à l'article 41 de la loi du 29 mars 2004 concernant la coopération avec la Cour pénale internationale et les tribunaux pénaux internationaux;

3° au livre II, titre Iter, du même Code;

4° à l'article 147 du même Code;

5° aux articles 160, 161, 162, 163, 168, 171, 173 et 176 du même Code;

6° aux articles 180 et 186 du même Code;

7° à l'article 210*bis* du même Code;

8° aux articles 246, 247, 248, 249 et 250 du même Code;

9° à l'article 259*bis* du même Code;

10° artikel 314*bis* van hetzelfde Wetboek;

11° de artikelen 324*bis* en 324*ter* van hetzelfde Wetboek;

12° de artikelen 327, 328, 329 of 330 van hetzelfde Wetboek, voor zover een klacht is ingediend;

13° artikel 331*bis* van hetzelfde Wetboek;

14° artikel 347*bis* van hetzelfde Wetboek;

15° de artikelen 372 tot 377*bis* van hetzelfde Wetboek;

16° artikel 377*quater* van hetzelfde Wetboek;

17° de artikelen 379, 380 en 383*bis*, § 1 en 3 van hetzelfde Wetboek;

18° artikel 393 van hetzelfde Wetboek;

19° de artikelen 394 of 397 van hetzelfde Wetboek;

20° de artikelen 428 en 429 van hetzelfde Wetboek;

21° artikel 433*bis*/1 van hetzelfde Wetboek;

22° de artikelen 433*quinquies* tot 433*octies* van hetzelfde Wetboek;

23° artikel 434 van hetzelfde Wetboek;

24° de artikelen 468, 470, 471 of 472 van hetzelfde Wetboek;

25° artikel 475 van hetzelfde Wetboek;

26° boek II, titel IX, hoofdstuk I, sectie 2*bis*, en hoofdstuk Ibis van hetzelfde Wetboek;

27° de artikelen 504*bis* en 504*ter* van hetzelfde Wetboek;

28° artikel 504*quater* van hetzelfde Wetboek;

29° artikel 505, eerste lid, 1° van hetzelfde Wetboek wanneer de betrokken zaken werden weggenomen, verduisterd of verkregen door een misdaad of wanbedrijf vermeld in dit artikel;

30° artikel 505, eerste lid, 2°, 3° en 4° van hetzelfde Wetboek;

31° de artikelen 510, 511, eerste lid of 516 van hetzelfde Wetboek;

10° à l'article 314*bis* du même Code;

11° aux articles 324*bis* et 324*ter* du même Code;

12° aux articles 327, 328, 329 ou 330 du même Code, pour autant qu'une plainte ait été déposée;

13° à l'article 331*bis* du même Code;

14° à l'article 347*bis* du même Code;

15° aux articles 372 à 377*bis* du même Code;

16° à l'article 377*quater* du même Code;

17° aux articles 379, 380 et 383*bis*, §§ 1er et 3, du même Code;

18° à l'article 393 du même Code;

19° aux articles 394 ou 397 du même Code;

20° aux articles 428 et 429 du même Code;

21° à l'article 433*bis*/1 du même Code;

22° aux articles 433*quinquies* à 433*octies* du même Code;

23° à l'article 434 du même Code;

24° aux articles 468, 470, 471 ou 472 du même Code;

25° à l'article 475 du même Code;

26° au livre II, titre IX, chapitre Ier, section 2*bis*, et chapitre Ier*bis* du même Code;

27° aux articles 504*bis* et 504*ter* du même Code;

28° à l'article 504*quater* du même Code;

29° à l'article 505, alinéa 1er, 1° du même Code lorsque les choses concernées ont été enlevées, détournées ou obtenues à l'aide d'un crime ou d'un délit visés au présent article;

30° à l'article 505, alinéa premier, 2°, 3° et 4° du même Code;

31° aux articles 510, 511, alinéa 1er, ou 516 du même Code;

32° artikel 520 van hetzelfde Wetboek, indien de omstandigheden bedoeld in de artikelen 510 of 511, eerste lid, van hetzelfde Wetboek verenigd zijn;

33° artikelen 550*bis* en 550*ter* van hetzelfde Wetboek;

34° artikel 2*bis* van de wet van 24 februari 1921 betreffende het verhandelen van giftstoffen, slaapmiddelen en verdovende middelen, psychotrope stoffen, ontsmettingsstoffen en antiseptica en van de stoffen die kunnen gebruikt worden voor de illegale vervaardiging van verdovende middelen en psychotrope stoffen;

35° artikel 145, § 3 en § 3*bis* van de wet van 13 juni 2005 betreffende de elektronische communicatie;

36° artikel 10 van de wet van 5 augustus 1991 betreffende de in-, uit- en doorvoer van wapens, munitie en speciaal voor militair gebruik dienstig materieel en daaraan verbonden technologie;

37° artikel 47 van het decreet van het Vlaams Parlement van 15 juni 2012 betreffende de in-, uit-, doorvoer en overbrenging van defensiegerelateerde producten, ander voor militair gebruik dienstig materiaal, ordehandhavingsmateriaal, civiele vuurwapens, onderdelen en munitie;

38° artikel 20 van het decreet van het Waals Gewest van 21 juni 2012 betreffende de invoer, uitvoer, doorvoer en overdracht van civiele wapens en van defensiegerelateerde producten;

39° artikel 42 van de ordonnantie van het Brussels Hoofdstedelijk gewest van 20 juni 2013 betreffende de in-, uit-, doorvoer en overbrenging van defensiegerelateerde producten, ander voor militair gebruik dienstig materiaal, ordehandhavingsmateriaal, civiele vuurwapens, onderdelen, toebehoren en munitie ervan;

40° artikelen 8 tot 11, 14, 16, 19, 1°, 2°, 3°, 5° en 6°, 20, 22, 27 en 33 van de wet van 8 juni 2006 houdende regeling van economische en individuele activiteiten met wapens, ook “wapenwet” genoemd;

41° de wet van 28 mei 1956 betreffende ontplofbare en voor de deflagratie vatbare stoffen en mengsels en de daarmede geladen tuigen;

42° artikelen 21 tot 26 van het Samenwerkingsakkoord tussen de Federale Staat, het Vlaams Gewest, het Waals Gewest en het Brussels Hoofdstedelijk Gewest betreffende de uitvoering van de overeenkomst tot verbod van de ontwikkeling, de productie, de aanleg

32° à l’article 520 du même Code, si les circonstances visées aux articles 510 ou 511, alinéa 1er, du même Code sont réunies;

33° aux articles 550*bis* et 550*ter* du même Code;

34° à l’article 2*bis* de la loi du 24 février 1921 concernant le trafic des substances vénéneuses, soporifiques, stupéfiantes, psychotropes, désinfectantes ou antiseptiques et des substances pouvant servir à la fabrication illicite de substances stupéfiantes et psychotropes;

35° à l’article 145, §§ 3 et 3*bis*, de la loi du 13 juin 2005 relative aux communications électroniques;

36° à l’article 10 de la loi du 5 août 1991 relative à l’importation, à l’exportation et au transit d’armes, de munitions et de matériel devant servir spécialement à un usage militaire et de la technologie y afférente;

37° à l’article 47 du décret du parlement flamand du 15 juin 2012 concernant l’importation, l’exportation, le transit et le transfert de produits liés à la défense, d’autre matériel à usage militaire, de matériel de maintien de l’ordre, d’armes à feu civiles, de pièces et de munitions;

38° à l’article 20 du décret de la Région wallonne du 21 juin 2012 relatif à l’importation, à l’exportation, au transit et au transfert d’armes civiles et de produits liés à la défense;

39° à l’article 42 de l’ordonnance de la Région de Bruxelles-Capitale du 20 juin 2013 relative à l’importation, à l’exportation, au transit et au transfert de produits liés à la défense, d’autre matériel pouvant servir à un usage militaire, de matériel lié au maintien de l’ordre, d’armes à feu à usage civil, de leurs pièces, accessoires et munitions;

40° aux articles 8 à 11, 14, 16, 19, 1°, 2°, 3°, 5° et 6°, 20, 22, 27 et 33 de la loi du 8 juin 2006 réglant des activités économiques et individuelles avec des armes, aussi appelée “Loi sur les armes”;

41° à la loi du 28 mai 1956 relative aux substances et mélanges explosibles ou susceptibles de déflagrer et aux engins qui en sont chargés;

42° aux articles 21 à 26 de l’Accord de Coopération du 2 mars 2007 entre l’État fédéral, la Région flamande, la Région wallonne et la Région de Bruxelles-Capitale relatif à l’exécution de la Convention sur l’interdiction de la mise au point, de la fabrication, du stockage et de

van voorraden en het gebruik van chemische wapens en inzake de vernietiging van deze wapens, gedaan te Parijs op 13 januari 1993;

43° de artikelen 77*bis* tot 77*quinquies* van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen;

44° artikel 10, § 1, 2°, van de wet van 15 juli 1985 betreffende het gebruik bij dieren van stoffen met hormonale, anti-hormonale, beta-adrenergische of productiestimulerende werking;

45° artikel 1 van het koninklijk besluit van 12 april 1974 betreffende sommige verrichtingen in verband met stoffen met hormonale, anti-hormonale, anabole, anti-infectieuze, anti-parasitaire, en anti-inflammatoire werking, welk artikel betrekking heeft op strafbare feiten waarop overeenkomstig de wet van 24 februari 1921 betreffende het verhandelen van de gifstoffen, slaapmiddelen en verdovende middelen, ontsmettingsstoffen en antiseptica straffen worden gesteld.";

3° in de paragrafen 3 en 4 wordt het woord "bewakingsmaatregel" telkens vervangen door het woord "maatregel";

4° paragraaf 5 wordt vervangen als volgt:

"§ 5. Ingeval van ontdekking op heterdaad en zolang de heterdaadsituatie duurt, kan de procureur des Konings de maatregel bedoeld in § 1 bevelen voor de strafbare feiten bedoeld in de artikelen 347*bis*, 434 of 470 van het Strafwetboek.";

5° in paragraaf 6, eerste lid, worden de woorden "tijdelijk privételecommunicatie afluisteren, er kennis van nemen en opnemen tijdens de overbrenging ervan" vervangen door de woorden "tijdelijk niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem onderscheppen, er kennis van nemen en opnemen".

Artikel 18

Artikel 90*quater* van hetzelfde Wetboek, ingevoegd bij de wet van 30 juni 1994 en laatstelijk gewijzigd bij de wet van 5 februari 2016, wordt vervangen als volgt:

"Art. 90*quater*. § 1. Tot iedere maatregel op grond van artikel 90*ter* verleent de onderzoeksrechter een schriftelijke voorafgaande met redenen omklede machtiging die hij meedeelt aan de procureur des Konings.

l'emploi des armes chimiques et sur leur destruction, faite à Paris le 13 janvier 1993;

43° aux articles 77*bis* à 77*quinquies* de la loi du 15 décembre 1980 concernant l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers;

44° à l'article 10, § 1er, 2°, de la loi du 15 juillet 1985 relative à l'utilisation de substances à effet hormonal, à effet antihormonal, à effet bêta-adrénergique ou à effet stimulateur de production chez les animaux;

45° article 1er de l'arrêté royal du 12 avril 1974 relatif à certaines opérations concernant les substances à action hormonale, antihormonale, anabolisante, bêta-adrénergique, anti-infectieuse, antiparasitaire et anti-inflammatoire, article précité visant des infractions punies conformément à la loi du 24 février 1921 concernant le trafic des substances vénéneuses, soporifiques, stupéfiantes, désinfectantes ou antiseptiques.";

3° aux paragraphes 3 et 4 les mots "mesures de surveillance" sont chaque fois remplacés par le mot "mesure";

4° le paragraphe 5 est remplacé par ce qui suit:

"§ 5. En cas de flagrant délit et tant que la situation de flagrant délit perdure, le procureur du Roi peut ordonner la mesure visée au § 1er pour les infractions visées aux articles 347*bis*, 434 ou 470 du Code pénal.";

5° au paragraphe 6, alinéa 1er, les mots "temporairement écouter, prendre connaissance et enregistrer, pendant leur transmission, des télécommunications privées" sont remplacés par les mots "intercepter, prendre connaissance et enregistrer des communications non accessibles au public ou des données d'un système informatique".

Article 18

L'article 90*quater* du même Code, inséré par la loi du 30 juin 1994 et modifié en dernier lieu par la loi du 5 février 2016, est remplacé par ce qui suit:

"Art. 90*quater*. § 1er. Toute mesure sur la base de l'article 90*ter* fait l'objet d'une autorisation écrite préalable et motivée du juge d'instruction, que celui-ci communique au procureur du Roi.

De machtiging wordt gedagtekend en vermeldt:

1° de aanwijzingen en de concrete feiten, eigen aan de zaak, die de maatregel wettigen overeenkomstig artikel 90*ter*;

2° de redenen waarom de maatregel onontbeerlijk is om de waarheid aan de dag te brengen;

3° de persoon, het communicatiemiddel, het informaticasysteem of de plaats die het voorwerp is van de bewaking;

4° de periode tijdens dewelke de maatregel kan worden uitgeoefend, die niet langer mag zijn dan één maand. Deze termijn vangt aan de dag van de machtiging waarbij de maatregel wordt bevolen, of, ingeval van artikel 90*quinquies*, eerste lid, verlengd, en loopt tot en met de dag voor de zoveelste van de daarop volgende maand;

5° de naam en de hoedanigheid van de officier of officieren van gerechtelijke politie aangewezen voor de uitvoering van de maatregel.

In spoedeisende gevallen kan de machtiging mondeling worden verleend. Deze machtiging moet uiterlijk binnen vierentwintig uren worden bevestigd in de vorm bepaald in het tweede lid.

§ 2. De onderzoeksrechter kan, om de maatregel bedoeld in artikel 90*ter*, § 1, mogelijk te maken, rechtstreeks of via de tussenkomst van een politiedienst aangewezen door de Koning, de medewerking vorderen van:

— de operator van een elektronisch communicatienetwerk, en

— iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.

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 aan de vorderingen bedoeld in de vorige leden weigert of niet

L'autorisation est datée et indique:

1° les indices ainsi que les faits concrets et propres à la cause qui justifient la mesure conformément à l'article 90*ter*;

2° les motifs pour lesquels la mesure est indispensable à la manifestation de la vérité;

3° la personne, le moyen de communication, le système informatique ou le lieu soumis à la surveillance;

4° la période pendant laquelle la mesure peut être exécutée et qui ne peut excéder un mois. Ce délai commence à courir le jour de l'autorisation ordonnant ou, dans le cas de l'article 90*quinquies*, alinéa 1er, prolongeant la mesure et s'achève la veille du quantième du mois suivant;

5° les nom et qualité de l'officier ou des officiers de police judiciaire commis pour l'exécution de la mesure.

En cas d'urgence, l'autorisation peut être donnée verbalement. Elle doit être confirmée dans la forme prévue à l'alinéa 2 au plus tard dans les vingt-quatre heures.

§ 2. Afin de permettre la mesure visée à l'article 90*ter*, § 1er, le juge d'instruction peut requérir, directement ou par l'intermédiaire d'un service de police désigné par le Roi, le concours:

— de l'opérateur d'un réseau de communications électroniques; et

— de toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.

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 aux alinéas précédents,

verleent in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, 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 euro tot twintigduizend euro.

§ 3. De onderzoeksrechter mag voor de tenuitvoerlegging van de maatregel bedoeld in artikel 90*ter*, § 1 alleen officieren van gerechtelijke politie aanwijzen. Deze kunnen zich echter laten bijstaan door agenten van gerechtelijke politie en, onder de voorwaarden door de Koning bepaald, door personeelsleden van het administratief en logistiek kader van de geïntegreerde politie. De laatstgenoemde personen mogen niet belast worden met de analyse van de inhoud van de opgenomen communicatie of gegevens, tenzij het een specifieke expertise betreft, of met de selectie van voor het onderzoek relevant geachte delen, zoals bedoeld in artikel 90*sexies*, § 1, 2°.

De officieren van gerechtelijke politie houden de namen bij van de personen door wie zij zich laten bijstaan, in een lijst die voor elk dossier afzonderlijk wordt opgesteld volgens de modaliteiten door de Koning bepaald, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer. Indien deze personen belast zijn met de uitvoering van het bevel bedoeld in artikel 90*ter*, § 1, derde lid, worden hun namen niet vermeld in het gerechtelijk dossier.

De aangewezen officieren van gerechtelijke politie brengen ten minste om de vijf dagen schriftelijk verslag uit aan de onderzoeksrechter over de tenuitvoerlegging van de beschikking.

§ 4. De onderzoeksrechter kan personen waarvan hij vermoedt dat ze een bijzondere kennis hebben van het communicatiemiddel of het informaticasysteem waarop de maatregel betrekking heeft of van diensten of toepassingen om gegevens, die worden opgeslagen, verwerkt of overgedragen via een communicatiemiddel of een informaticasysteem, te beveiligen, te coderen of te versleutelen, rechtstreeks of via de tussenkomst van een politiedienst aangewezen door de Koning, vorderen inlichtingen te verlenen over de werking ervan en over de wijze om in een verstaanbare vorm toegang te verkrijgen tot de inhoud ervan die wordt of is overgebracht.

Hij kan personen vorderen om deze inhoud toegankelijk te maken in de door hem gewenste vorm.

Iedere persoon die zijn technische medewerking weigert aan de vorderingen bedoeld in de vorige leden, wordt gestraft met gevangenisstraf van zes maanden

concours dont les modalités sont fixées par le Roi, sur la proposition du ministre de la Justice et du ministre compétent pour les Télécommunications, ou ne le prête pas en temps réel ou, le cas échéant, au moment précisé dans la réquisition, est punie d'une amende de vingt-six euros à vingt mille euros.

§ 3. Le juge d'instruction ne peut commettre pour l'exécution de la mesure visée à l'article 90*ter*, § 1er, que des officiers de police judiciaire. Ceux-ci peuvent néanmoins se faire assister par des agents de police judiciaire et, selon les conditions fixées par le Roi, par des agents du cadre administratif et logistique de la police intégrée. Ces dernières personnes ne peuvent être chargées de l'analyse du contenu des communications ou données enregistrées, sauf s'il s'agit d'une expertise spécifique, ou de la sélection des parties estimées pertinentes pour l'instruction, comme prévu à l'article 90*sexies*, § 1er, 2°.

Les officiers de police judiciaire conservent les noms des personnes qui peuvent les assister dans une liste établie séparément pour chaque dossier selon les modalités fixées par le Roi, après avis de la Commission pour la protection de la vie privée. Si ces personnes sont chargées de l'exécution de l'ordonnance visée à l'article 90*ter*, § 1er, alinéa 3, leur nom n'est pas mentionné dans le dossier judiciaire.

Les officiers de police judiciaire commis font rapport par écrit au moins tous les cinq jours au juge d'instruction sur l'exécution de l'ordonnance.

§ 4. Le juge d'instruction peut exiger, directement ou par le l'intermédiaire d'un service de police désigné par le Roi, de personnes dont il présume qu'elles ont une connaissance particulière du moyen de communication ou du système informatique qui fait l'objet de la mesure ou de services ou applications qui permettent de protéger, de coder ou de crypter les données qui sont stockées, traitées ou transmises par un moyen de communication ou un système informatique, qu'elles fournissent des informations sur le fonctionnement de ce moyen ou système et sur la manière d'accéder à son contenu qui est ou a été transmis, dans une forme compréhensible.

Il peut ordonner aux personnes de rendre accessible ce contenu, dans la forme qu'il aura souhaitée.

Toute personne qui refuse de prêter son concours technique aux réquisitions visées aux alinéas précédents est punie d'un emprisonnement de six mois à

tot een jaar en met geldboete van zesentwintig euro tot twintigduizend euro of met een van die straffen alleen.

Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of gevorderd wordt zijn technische medewerking te verlenen, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

§ 5. In voorkomend geval is artikel 39*bis*, § 3, vierde lid toepasbaar op de gegevens, aangetroffen door een zoeking in een informaticasysteem met toepassing van artikel 90*ter*, § 1.".

Artikel 19

In artikel 90*quinquies* van hetzelfde Wetboek, ingevoegd bij de wet van 30 juni 1994, worden de volgende wijzigingen aangebracht:

1° het eerste lid wordt vervangen als volgt:

"De onderzoeksrechter kan de uitwerking van de machtiging bedoeld in artikel 90*quater*, § 1, één of meer malen verlengen met een termijn die niet langer mag zijn dan één maand, met een maximum van zes maanden, onverminderd zijn beslissing om aan de maatregel een einde te maken zodra de omstandigheden die deze gewettigd hebben, verdwenen zijn. Deze termijn van zes maanden vangt aan de dag van de eerste machtiging waarbij de maatregel wordt bevolen, en loopt tot en met de dag voor de zoveelste van de zesde daarop volgende maand. Indien de maatregel, wegens de technische voorbereiding ervan, daadwerkelijk werd aangevat op een latere dag dan deze van de eerste machtiging, vangt de termijn van zes maanden aan de dag van deze daadwerkelijke aanvatting en ten laatste twee maanden na de dag van de eerste machtiging.";

2° in het tweede en het derde lid wordt het woord "beschikking" telkens vervangen door het woord "machtiging".

Artikel 20

Artikel 90*sexies* van hetzelfde Wetboek, ingevoegd bij de wet van 30 juni 1994 en gewijzigd bij de wetten van 10 juni 1998 en 5 februari 2016, wordt vervangen als volgt:

"§ 1. De aangewezen officieren van gerechtelijke politie stellen aan de onderzoeksrechter ter beschikking:

un an et d'une amende de vingt-six euros à vingt mille euros ou d'une de ces peines seulement.

Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou est requise d'y prêter son concours technique, est tenue au secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

§ 5. Le cas échéant, l'article 39*bis*, § 3, alinéa 4, est applicable aux données recueillies par une recherche dans un système informatique en application de l'article 90*ter*, § 1er.".

Article 19

A l'article 90*quinquies* du même Code, inséré par la loi du 30 juin 1994, les modifications suivantes sont apportées:

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

"Le juge d'instruction peut prolonger une ou plusieurs fois les effets de son autorisation visée à l'article 90*quater*, § 1er, pour un nouveau terme qui ne peut dépasser un mois, avec un maximum de six mois, sans préjudice de sa décision de mettre fin à la mesure dès que les circonstances qui l'ont justifiée ont disparu. Ce délai de six mois commence à courir le jour de la première autorisation ordonnant la mesure et s'achève la veille du quantième du sixième mois suivant. Si la mesure, en raison de sa préparation technique, a effectivement débuté un jour postérieur à celui de la première autorisation, ce délai de six mois commence à courir au moment de ce début effectif et au plus tard deux mois après le jour de la première autorisation.";

2° dans les alinéas 2 et 3, le mot "ordonnance" est chaque fois remplacé par le mot "autorisation".

Article 20

L'article 90*sexies* du même Code, inséré par la loi du 30 juin 1994 et modifié par les lois du 10 juin 1998 et 5 février 2016, est remplacé par ce qui suit:

"§ 1er. Les officiers de police judiciaire commis mettent à la disposition du juge d'instruction:

1° Het bestand bevattende de opgenomen niet voor publiek toegankelijke communicaties of gegevens van een informaticasysteem bekomen als gevolg van de maatregelen genomen met toepassing van de artikelen 90*ter*, 90*quater* en 90*quinquies*;

2° De overschrijving of weergave van de door de aangewezen officieren van gerechtelijke politie voor het onderzoek van belang geachte gedeelten van de opgenomen communicaties of gegevens, en de eventuele vertaling ervan;

3° In voorkomend geval, de plaats van de gegevens, bedoeld in 2°, in het informaticasysteem;

4° Een algemene beschrijving van de inhoud en van de identificatiegegevens van de gebruikte communicatiemiddelen of informaticasystemen wat betreft de niet van belang geachte communicaties of gegevens.

§ 2. Onverminderd de selectie door de officieren van gerechtelijke politie bedoeld in § 1, beoordeelt de onderzoeksrechter welke gedeelten van alle opgenomen niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem van belang zijn voor het onderzoek. In zoverre deze gedeelten van de communicatie of gegevens niet overgeschreven, weergegeven of vertaald zijn overeenkomstig § 1, moeten zij bijkomend overgeschreven, weergegeven en eventueel vertaald worden. De onderzoeksrechter laat daarvan proces-verbaal opmaken.

§ 3. De niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem die onder het beroepsgeheim vallen, worden niet opgetekend in het proces-verbaal. Deze communicatie of gegevens worden in een bestand onder verzegelde omslag neergelegd ter griffie. Gaat het om personen bedoeld in artikel 90*octies*, dan wordt ter zake gehandeld zoals bepaald in dat artikel.

§ 4. De machtigingen van de onderzoeksrechter, de verslagen van de officieren van gerechtelijke politie bedoeld in artikel 90*quater*, § 3, en de processen-verbaal die betrekking hebben op de tenuitvoerlegging van de maatregel, worden uiterlijk na het beëindigen van de maatregelen bij het dossier gevoegd.”.

Artikel 21

Artikel 90*septies* van hetzelfde Wetboek, ingevoegd bij de wet van 30 juni 1994 en gewijzigd bij de wetten van 10 juni 1998, 28 november 2000 en 5 februari 2016, wordt vervangen als volgt:

1° le fichier contenant les communications non accessibles au public ou les données d’un système informatique enregistrées et obtenues à la suite des mesures prises en application des articles 90*ter*, 90*quater* et 90*quinquies*;

2° la transcription ou reproduction des parties des communications ou données enregistrées estimées pertinentes pour l’instruction par les officiers de police judiciaire commis, et leur traduction éventuelle;

3° le cas échéant, l’endroit où se trouvent les données visées au 2° dans le système informatique;

4° Une description générale du contenu et des données d’identification des moyens de communication ou systèmes informatiques utilisés en ce qui concerne les communications ou données estimées non pertinentes.

§ 2. Sans préjudice de la sélection par les officiers de police judiciaire visés au § 1er, le juge d’instruction apprécie parmi toutes les communications non accessibles au public ou données d’un système informatique qui ont été enregistrées les parties qui sont pertinentes pour l’instruction. Dans la mesure où ces parties de communications ou données n’ont pas été transcrites, reproduites ou traduites conformément au § 1er, elles seront transcrites, reproduites et éventuellement traduites. Le juge d’instruction en fait dresser procès-verbal.

§ 3. Les communications non accessibles au public ou données d’un système informatique qui sont couvertes par le secret professionnel ne sont pas consignées dans le procès-verbal. Ces communications ou données sont déposées au greffe dans un fichier sous pli scellé. S’il s’agit de personnes visées à l’article 90*octies*, on procède ainsi qu’il est prévu à cet article.

§ 4. Les autorisations du juge d’instruction, les rapports des officiers de police judiciaire visés à l’article 90*quater*, § 3, et les procès-verbaux relatifs à l’exécution de la mesure, sont joints au dossier au plus tard après qu’il est mis fin à la mesure.”.

Article 21

L’article 90*septies* du même Code, inséré par la loi du 30 juin 1994 et modifié par les lois du 10 juin 1998, 28 novembre 2000 et 5 février 2016, est remplacé par ce qui suit:

"Art. 90*septies*. § 1. De passende middelen worden aangewend om de integriteit en de vertrouwelijkheid van de opgenomen niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem te waarborgen.

§ 2. Ieder bestand bevat het onderwerp van de opgenomen niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem en de dagen en uren waarop de maatregel is uitgevoerd.

§ 3. Iedere aantekening in het kader van de tenuitvoerlegging van de maatregelen bedoeld in de artikelen 90*ter*, 90*quater* en 90*quinquies* door de daartoe aangewezen personen, die niet is opgetekend in een proces-verbaal, wordt vernietigd, met uitzondering van het vermelde in artikel 90*sexies*, § 1, 2°, 3° en 4° en onverminderd artikel 33 van de wet van … betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecommunicaties. De voor de uitvoering van de maatregel aangewezen officieren van gerechtelijke politie gaan over tot deze vernietiging en vermelden dit in een proces-verbaal.

Om beheersredenen en om aan de verplichting van artikel 90*decies* te kunnen voldoen, kunnen de strikt noodzakelijke administratieve gegevens evenwel bewaard blijven bij de dienst aangewezen door de Koning.

§ 4. De bestanden bedoeld in artikel 90*sexies*, § 1, 1° worden bewaard onder verzegelde omslag ter griffie. Ze kunnen bovendien ook worden bewaard bij de dienst aangewezen door de Koning onder de voorwaarden en modaliteiten door Hem bepaald na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer.

De stukken bedoeld in artikel 90*sexies*, § 1, 2°, 3° en 4° en de afschriften van de processen-verbaal worden onder verzegelde omslag ter griffie bewaard.

§ 5. De griffier vermeldt in een per dag bijgehouden, bijzonder register:

1° de dag van de neerlegging van de in artikel 90*sexies*, § 1 bedoelde bestanden en stukken, alsmede van ieder afschrift van proces-verbaal;

2° de naam van de onderzoeksrechter die de maatregelen heeft bevolen of bevestigd en het voorwerp ervan;

3° de dag waarop de zegels zijn verbroken en in voorkomend geval opnieuw zijn gelegd;

"Art. 90*septies*. § 1er. Les moyens appropriés sont utilisés pour garantir l'intégrité et la confidentialité des communications non accessibles au public ou données d'un système informatique qui ont été enregistrées.

§ 2. Chaque fichier contient le sujet des communications non accessibles au public ou données d'un système informatique qui ont été enregistrées ainsi que les jours et heures auxquels la mesure a été exécutée.

§ 3. Toute note prise dans le cadre de l'exécution des mesures visées aux articles 90*ter*, 90*quater* et 90*quinquies* par les personnes commises à cette fin qui n'est pas consignée dans un procès-verbal, est détruite, à l'exception de ce qui est mentionné à l'article 90*sexies*, § 1er, 2°, 3° et 4°, et sans préjudice de l'article 33 de la loi du … relative à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications. Les officiers de police judiciaire commis pour l'exécution de la mesure procèdent à cette destruction et en font mention dans un procès-verbal.

Pour des raisons de gestion et en vue du respect de l'obligation de l'article 90*decies*, les données administratives strictement nécessaires peuvent néanmoins être conservées au sein du service désigné par le Roi.

§ 4. Les fichiers visés à l'article 90*sexies*, § 1er, 1°, sont conservés au greffe sous pli scellé. Ils peuvent en outre être conservés au sein du service désigné par le Roi aux conditions et modalités fixées par Lui après avis de la Commission de la protection de la vie privée.

Les pièces visées à l'article 90*sexies*, § 1er, 2°, 3° et 4°, et les copies des procès-verbaux sont conservées au greffe sous pli scellé.

§ 5. Le greffier mentionne dans un registre spécial tenu journellement:

1° le jour du dépôt des fichiers et pièces visés à l'article 90*sexies*, § 1er, ainsi que de chaque copie de procès-verbal;

2° le nom du juge d'instruction qui a ordonné ou confirmé la mesure et l'objet de celle-ci;

3° le jour où les scellés sont ouverts et éventuellement réapposés;

4° de datum van de kennisname van de in artikel 90*sexies*, § 1 bedoelde bestanden en stukken, van de afschriften van processen-verbaal, alsook de namen van de personen er kennis van genomen hebben;

5° iedere andere gebeurtenis die erop betrekking heeft.

§ 6. De inverdenkinggestelde, de beklaagde, de burgerlijke partij of hun raadsman ontvangen op eenvoudig verzoek een kopie van het geheel van de opgenomen niet voor het publiek toegankelijke communicaties of gegevens van een informaticasysteem, waarvan bepaalde van belang geachte gedeelten overgeschreven of weergegeven werden en opgenomen werden in een proces-verbaal waarvan ze inzage hebben.

De inverdenkinggestelde, de beklaagde, de burgerlijke partij of hun raadsman kunnen de rechter verzoeken om de overeenkomstig § 4 ter griffie neergelegde andere bestanden of stukken ter griffie te raadplegen, en bijkomende delen van de opgenomen communicatie of gegevens over te schrijven of weer te geven. Het verzoek dat gericht is tot de onderzoeksrechter, wordt behandeld overeenkomstig artikel 61*quinquies*.

De rechter kan het verzoek afwijzen indien hij de raadpleging of de overschrijving of weergave van bijkomende delen niet noodzakelijk acht om de waarheid aan de dag te brengen, indien hij dit op dat ogenblik nadelig acht voor het onderzoek, of om redenen die verband houden met de bescherming van andere rechten of belangen van personen. Hij kan de raadpleging of de overschrijving of weergave van bijkomende delen ook beperken tot een door hem nader omschreven selectie van bestanden of stukken.”.

Artikel 22

Artikel 90*octies* van hetzelfde Wetboek, ingevoegd bij de wet van 30 juni 1994, wordt vervangen als volgt:

“Art. 90*octies*. § 1. De maatregel kan alleen betrekking hebben op de lokalen aangewend voor beroepsdoeleinden, de woonplaats, de communicatiemiddelen of de informaticasystemen van een advocaat of een arts, indien deze er zelf van verdacht worden een van de strafbare feiten bedoeld in artikel 90*ter* te hebben gepleegd of eraan deelgenomen te hebben, of, indien precieze feiten doen vermoeden dat derden die ervan verdacht worden een van de strafbare feiten bedoeld in artikel 90*ter* te hebben gepleegd, gebruik maken van diens lokalen, woonplaats, communicatiemiddelen of informaticasystemen.

4° la date de prise de connaissance des fichiers et pièces visés à l’article 90*sexies*, § 1er, des copies des procès-verbaux, ainsi que le nom des personnes qui en ont pris connaissance;

5° tous les autres événements qui s’y rapportent.

§ 6. L’inculpé, le prévenu, la partie civile ou leurs conseils reçoivent, sur simple demande, copie de la totalité des communications non accessibles au public ou données d’un système informatique, dont certaines parties estimées pertinentes ont été transcrites ou reproduites et consignées dans un procès-verbal qu’ils ont le droit de consulter.

L’inculpé, le prévenu, la partie civile ou leurs conseils peuvent demander au juge d’instruction de consulter au greffe les autres fichiers ou pièces déposés conformément au § 4 au greffe, ainsi que de transcrire ou reproduire des parties supplémentaires des communications ou données enregistrées. La demande, adressée au juge d’instruction, est traitée conformément à l’article 61*quinquies*.

Le juge d’instruction peut en outre rejeter cette demande s’il estime que la consultation, la transcription ou la reproduction des parties supplémentaires n’est pas nécessaire à la manifestation de la vérité, s’il le juge à ce moment préjudiciable à l’enquête ou pour des raisons liées à la protection d’autres droits ou intérêts de personnes. Il peut également limiter la consultation ou la transcription ou reproduction de parties supplémentaires à une sélection de fichiers ou pièces qu’il détermine.”.

Article 22

L’article 90*octies* du même Code, inséré par la loi du 30 juin 1994, est remplacé par ce qui suit:

“Art. 90*octies*. § 1er. La mesure ne pourra porter sur les locaux utilisés à des fins professionnelles, la résidence, les moyens de communication ou les systèmes informatiques d’un avocat ou d’un médecin que si celui-ci est lui-même soupçonné d’avoir commis une des infractions visées à l’article 90*ter* ou d’y avoir participé, ou si des faits précis laissent présumer que des tiers soupçonnés d’avoir commis une des infractions visées à l’article 90*ter*, utilisent ses locaux, sa résidence, ses moyens de communication ou ses systèmes informatiques.

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

Deze personen zijn tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

§ 3. De onderzoeksrechter beoordeelt, na overleg met de stafhouder of de vertegenwoordiger van de provinciale orde van geneesheren, welke gedeelten van de in artikel 90*sexies*, § 3, bedoelde niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem, die hij van belang acht voor het onderzoek, onder het beroepsgeheim vallen en welke niet.

Enkel de gedeelten van de communicatie of gegevens bedoeld in het vorige lid die worden geacht niet onder het beroepsgeheim te vallen, worden overgeschreven of weergegeven en worden desgevallend vertaald. De onderzoeksrechter laat hiervan proces-verbaal opmaken. De bestanden bevattende deze communicatie of gegevens worden onder verzegelde omslag neergelegd ter griffie.

Alle overige communicatie of gegevens worden in een ander bestand onder afzonderlijke verzegelde omslag neergelegd ter griffie.".

Artikel 23

Artikel 90*novies* van hetzelfde Wetboek, ingevoegd bij de wet van 30 juni 1994 en gewijzigd bij de wet van 19 december 2002, wordt aangevuld met de woorden ", tenzij diens identiteit of woonplaats redelijkerwijze niet achterhaald kan worden.".

Artikel 24

In 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, 6 januari 2003 en xxx (dataretentiewet), wordt het derde lid vervangen als volgt:

"Hij brengt tegelijkertijd verslag uit over de toepassing van de artikelen 40*bis*, 46*ter*, 46*quater*, 46*quinquies*, 47*ter* tot 47*decies*, 56*bis*, 86*bis*, 86*ter*, 88*sexies*, en 89*ter*.".

§ 2. 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 personnes sont tenues au secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

§ 3. Le juge d'instruction évalue, après concertation avec le bâtonnier ou le représentant de l'ordre provincial des médecins, quelles parties des communications non accessibles au public ou données d'un système informatique visées à l'article 90*sexies*, § 3, qu'il estime pertinentes pour l'instruction, relèvent du secret professionnel et quelles sont celles qui n'en relèvent pas.

Seules les parties des communications ou données visées à l'alinéa précédent qui sont estimées ne pas relever du secret professionnel sont transcrites ou reproduites et, le cas échéant, traduites. Le juge d'instruction en fait dresser procès-verbal. Les fichiers contenant ces communications ou données sont déposés au greffe sous pli scellé.

Toutes les autres communications ou données sont déposées au greffe dans un autre fichier sous pli scellé séparé.".

Article 23

L'article 90*novies* du même Code, inséré par la loi du 30 juin 1994 et modifié par la loi du 19 décembre 2002, est complété par les mots ", sauf si son identité ou son adresse ne peut être raisonnablement retrouvée.".

Article 24

A 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, 6 janvier 2003 et xxx (loi data retention), l'alinéa 3 est remplacé par ce qui suit:

"Il fait en même temps rapport sur l'application des articles 40*bis*, 46*ter*, 46*quater*, 46*quinquies*, 47*ter* à 47*decies*, 56*bis*, 86*bis*, 86*ter*, 88*sexies* et 89*ter*.".

Artikel 25

In artikel 235*ter* van hetzelfde Wetboek, ingevoegd bij de wet van 27 december 2005 en gewijzigd bij de wetten van 16 januari 2009, 29 januari 2016 en 5 februari 2016, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1 wordt het eerste lid aangevuld met de woorden ", en over de toepassing van de maatregel bedoeld in artikel 46*sexies* indien daarbij een vertrouwelijk dossier werd aangelegd.";

2° in paragraaf 1, tweede lid, worden de woorden "en van de maatregel bedoeld in artikel 46*sexies*" ingevoegd tussen de woorden "observatie en infiltratie" en de woorden "bij het afsluiten van het opsporingsonderzoek";

3° in paragraaf 1, derde lid, worden de woorden "en van de maatregel bedoeld in artikel 46*sexies*" ingevoegd tussen de woorden "observatie en infiltratie" en de woorden "die werden toegepast";

4° in paragraaf 2 worden het vierde en het vijfde lid vervangen als volgt:

"Zij kan, met betrekking tot de toegepaste bijzondere opsporingsmethoden observatie en infiltratie en de maatregel bedoeld in artikel 46*sexies*, de onderzoeksrechter, de in de artikelen 47*sexies*, § 3, 6° en 47*octies*, § 3, 6° bedoelde officier van gerechtelijke politie, en de officier van gerechtelijke politie belast met de leiding over de uitvoering van de maatregel bedoeld in artikel 46*sexies*, afzonderlijk en buiten de aanwezigheid van de partijen horen.

De kamer van inbeschuldigingstelling kan de onderzoeksrechter gelasten de politieambtenaren die belast zijn met de uitvoering van de observatie en infiltratie, en de in artikel 47*octies*, § 1, tweede lid, bedoelde burger, de politieambtenaren belast met de uitvoering van de maatregel bedoeld in artikel 46*sexies*, en de in artikel 46*sexies*, § 1, tweede lid bedoelde burger te horen met toepassing van de artikelen 86*bis* en 86*ter*. Zij kan beslissen bij het verhoor door de onderzoeksrechter aanwezig te zijn of één van haar leden daartoe af te vaardigen.";

5° in paragraaf 3, eerste lid, worden de woorden "de artikelen 47*septies*, § 1, tweede lid, of 47*novies*, § 1, tweede lid," vervangen door de woorden "de artikelen 46*sexies*, § 3, zevende lid, 47*septies*, § 1, tweede lid, of 47*novies*, § 1, tweede lid,";

6° in paragraaf 4 worden de woorden "de observatie of infiltratie en de in artikel 47*octies*, § 1, tweede lid, bedoelde burger" vervangen door de woorden "de

Article 25

A l'article 235*ter* du même Code, inséré par la loi du 27 décembre 2005 et modifié par les lois du 16 janvier 2009, 29 janvier 2016 et 5 février 2016, les modifications suivantes sont apportées:

1° dans le paragraphe 1er, l'alinéa 1 est complété par les mots "et l'application de la mesure visée à l'article 46*septies* si un dossier confidentiel a été ouvert dans ce cadre.";

2° dans le paragraphe 1, l'alinéa 2 est complété par les mots "et de la mesure visée à l'article 46*sexies*.";

3° dans le paragraphe 1, l'alinéa 3, les mots "et de la mesure visée à l'article 46*sexies*" sont insérés entre les mots "d'observation et d'infiltration" et les mots "qui ont été appliquées";

4° dans le paragraphe 2, les alinéas 4 et 5 sont remplacés par ce qui suit:

"Pour les méthodes particulières de recherche d'observation et d'infiltration et la mesure visée à l'article 46*sexies*, elle peut entendre, séparément et en l'absence des parties, le juge d'instruction et l'officier de police judiciaire visé aux articles 47*sexies*, § 3, 6°, et 47*octies*, § 3, 6°, et l'officier de police judiciaire chargé de diriger la mise en œuvre de la mesure visée à l'article 46*sexies*.

La chambre des mises en accusation peut charger le juge d'instruction d'entendre les fonctionnaires de police chargés d'exécuter l'observation et l'infiltration, le civil visé à l'article 47*octies*, § 1er, alinéa 2, en application des articles 86*bis* et 86*ter*, les fonctionnaires de police chargés de la mise en œuvre de la mesure visée à l'article 46*sexies* et le civil visé à l'article 46*sexies*, § 1er, alinéa 2. Elle peut décider d'être présente à l'audition menée par le juge d'instruction ou de déléguer un de ses membres à cet effet.";

5° dans le paragraphe 3, l'alinéa 1er les mots "aux articles 47*septies*, § 1er, alinéa 2, ou 47*novies*, § 1er, alinéa 2," sont remplacés par les mots "aux articles 46*sexies*, § 3, alinéa 7, 47*septies*, § 1er, alinéa 2, ou 47*novies*, § 1er, alinéa 2,";

6° dans le paragraphe 4 les mots "de l'observation ou de l'infiltration et du civil visé à l'article 47*octies*, § 1er, alinéa 2" sont remplacés par les mots "de l'observation,

observatie, de infiltratie of de maatregel bedoeld in artikel 46*sexies*, en de in de artikelen 47*octies*, § 1, tweede lid en 46*sexies*, § 1, tweede lid bedoelde burger".

Artikel 26

In artikel 235*quater* van hetzelfde Wetboek, ingevoerd bij de wet van 27 december 2005, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1, eerste lid, worden de woorden "en van de maatregel bedoeld in artikel 46*sexies* indien daarbij een vertrouwelijk dossier werd aangelegd," ingevoegd tussen de woorden "observatie en infiltratie" en de woorden "die werden toegepast";

2° in paragraaf 1, tweede lid, worden de woorden "over de dossiers waarvoor tot observaties en infiltraties werd beslist door het openbaar ministerie of door de onderzoeksrechter" vervangen door de woorden "over de dossiers waarvoor door het openbaar ministerie of door de onderzoeksrechter werd beslist tot observaties en infiltraties en tot de maatregel bedoeld in artikel 46*sexies* indien daarbij een vertrouwelijk dossier werd aangelegd";

3° paragraaf 2, tweede lid, wordt vervangen als volgt:

"Zij kan, met betrekking tot de toegepaste bijzondere opsporingsmethoden observatie of infiltratie en de maatregel bedoeld in artikel 46*sexies*, de onderzoeksrechter, de in de artikelen 47*sexies*, § 3, 6°, en 47*octies*, § 3, 6°, bedoelde officier van gerechtelijke politie en de officier van gerechtelijke politie belast met de leiding over de uitvoering van de maatregel bedoeld in artikel 46*sexies* afzonderlijk en buiten de aanwezigheid van de partijen horen.";

4° in paragraaf 3, eerste lid, worden de woorden "de artikelen 47*septies*, § 1, tweede lid, of 47*novies*, § 1, tweede lid" vervangen door de woorden "de artikelen 47*septies*, § 1, tweede lid, 47*novies*, § 1, tweede lid of 46*sexies*, § 3, zevende lid";

5° in paragraaf 4 worden de woorden "de observatie of infiltratie en de in artikel 47*octies*, § 1, tweede lid, bedoelde burger" vervangen door de woorden "de observatie, de infiltratie of de maatregel bedoeld in artikel 46*sexies*, en de in de artikelen 47*octies*, § 1, tweede lid en 46*sexies*, § 1, tweede lid bedoelde burger".

de l'infiltration ou de la mesure visée à l'article 46*sexies*, et du civil visé aux articles 47*octies*, § 1er, alinéa 2, et 46*sexies*, § 1er, alinéa 2".

Article 26

A l'article 235*quater* du même Code, inséré par la loi du 27 décembre 2005, les modifications suivantes sont apportées:

1° dans le paragraphe 1er, l'alinéa 1er, les mots "et de la mesure visée à l'article 46*sexies* si un dossier confidentiel a été ouvert dans ce cadre," sont insérés entre les mots "d'observation et d'infiltration" et les mots "qui ont été appliquées";

2° dans le paragraphe 1, l'alinéa 2, les mots "pour lesquels des observations et des infiltrations ont été décidées par le ministère public ou par le juge d'instruction" sont remplacés par les mots "pour lesquels des observations et des infiltrations et la mesure visée à l'article 46*sexies*, si un dossier confidentiel a été ouvert dans ce cadre, ont été décidées par le ministère public ou par le juge d'instruction";

3° paragraphe 2, l'alinéa 2, est remplacé par ce qui suit:

"Pour les méthodes particulières de recherche d'observation ou d'infiltration et la mesure visée à l'article 46*sexies*, elle peut entendre, séparément et en l'absence des parties, le juge d'instruction et l'officier de police judiciaire visé aux articles 47*sexies*, § 3, 6°, et 47*octies*, § 3, 6°, et l'officier de police judiciaire chargé de diriger la mise en œuvre de la mesure visée à l'article 46*sexies*.";

4° dans le paragraphe 3, alinéa 1er, les mots "aux articles 47*septies*, § 1er, alinéa 2, ou 47*novies*, § 1er, alinéa 2" sont remplacés par les mots "aux articles 47*septies*, § 1er, alinéa 2, 47*novies*, § 1er, alinéa 2, ou 46*sexies*, § 3, alinéa 7";

5° dans le paragraphe 4 les mots "de l'observation ou de l'infiltration et du civil visé à l'article 47*octies*, § 1er, alinéa 2" sont remplacés par les mots "de l'observation, de l'infiltration ou de la mesure visée à l'article 46*sexies*, et du civil visé aux articles 47*octies*, § 1er, alinéa 2, et 46*sexies*, § 1er, alinéa 2".

Artikel 27

In artikel 464/13 van hetzelfde Wetboek, ingevoegd bij de wet van 11 februari 2014 worden de volgende wijzigingen aangebracht:

1° paragraaf 1 wordt vervangen als volgt:

"§ 1. De SUO-magistraat of de gevorderde politiedienst kan bij een schriftelijke en met redenen omklede beslissing, van de actoren bedoeld in het tweede lid de mededeling van de volgende inlichtingen vorderen:

1° de identificatie van een abonnee of een gewoonlijke gebruiker van een dienst zoals bedoeld in het tweede lid, tweede streepje, of van het gebruikte elektronische communicatiemiddel;

2° de identificatie van de diensten zoals bedoeld in het tweede lid, tweede streepje, waarop een bepaalde persoon geabonneerd is of die door een bepaalde persoon gewoonlijk worden gebruikt.

De volgende actoren zijn gehouden tot medewerking overeenkomstig het vorige lid:

— de operator van een elektronisch communicatienetwerk; en

— iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.";

2° paragraaf 2 wordt vervangen als volgt:

"§ 2. De actoren bedoeld in § 1, tweede lid, verstrekken alle beschikbare inlichtingen in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de beslissing, volgens de modaliteiten die bepaald worden bij het ter uitvoering van artikel 46*bis*, § 2, eerste en tweede lid, genomen koninklijk besluit.

Iedere persoon die de gegevens weigert mee te delen of deze niet meedeelt in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de beslissing, wordt gestraft met geldboete van zesentwintig euro tot tienduizend euro."

Article 27

A l'article 464/13 du même Code, inséré par la loi de 11 février 2014, les modifications suivantes sont apportées:

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

"§ 1er. Le magistrat EPE ou le service de police requis peut, par décision écrite et motivée, requérir les acteurs visés à l'alinéa 2 de lui communiquer les renseignements suivants:

1° l'identification d'un abonné ou d'un utilisateur habituel d'un service visé à l'alinéa 2, deuxième tiret, ou bien du moyen de communication électronique utilisé;

2° l'identification des services visés à l'alinéa 2, deuxième tiret, auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée.

Les acteurs suivants sont tenus de collaborer conformément à l'alinéa précédent:

— l'opérateur d'un réseau de communications électroniques; et

— toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.";

2° le paragraphe 2 est remplacé par ce qui suit:

"§ 2. Les acteurs visés au § 1er, alinéa 2, fournissent tous les renseignements disponibles en temps réel ou, le cas échéant, au moment précisé dans la décision, selon les modalités fixées par l'arrêté royal pris en exécution de l'article 46*bis*, § 2, alinéas 1er et 2.

Toute personne qui refuse de communiquer les données ou qui ne les communique pas en temps réel ou, le cas échéant, au moment précisé dans la réquisition est punie d'une amende de vingt-six euros à dix mille euros.".

Artikel 28

In artikel 464/25 van hetzelfde Wetboek, ingevoegd bij de wet van 11 februari 2014 worden de volgende wijzigingen aangebracht:

1° in paragraaf 1, eerste lid, worden de woorden "een operator van een elektronisch communicatienetwerk of de verstrekker van een elektronische communicatiedienst" vervangen door de woorden "de actoren bedoeld in het tweede lid";

2° in paragraaf 1 wordt tussen het eerste en het tweede lid een lid ingevoegd, luidende:

"De volgende actoren zijn gehouden tot medewerking overeenkomstig het vorige lid:

— de operator van een elektronisch communicatienetwerk; en

— iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.";

3° paragraaf 2 wordt vervangen als volgt:

"§ 2. De actoren bedoeld in § 1, tweede lid delen de gevorderde inlichtingen mee in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de beslissing, volgens de modaliteiten die bepaald worden bij het ter uitvoering van artikel 88*bis*, § 2, eerste en derde lid, genomen koninklijk besluit.

Iedere persoon die zijn technische medewerking aan de in dit artikel bedoelde vorderingen weigert of niet verleent in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de beslissing, wordt gestraft met een geldboete van zesentwintig euro tot tienduizend euro.".

TITEL 3

Bepalingen tot wijziging van het Strafwetboek

Artikel 29

In het Strafwetboek wordt het opschrift van Boek 2, Titel IV, Hoofdstuk V*bis* vervangen als volgt:

Article 28

A l'article 464/25 du même Code, inséré par la loi de 11 février 2014 les modifications suivantes sont apportées:

1° dans le paragraphe 1, alinéa 1, les mots "un opérateur d'un réseau de communication électronique ou le fournisseur d'un service de communication électronique" sont remplacés par les mots "les acteurs visés à l'alinéa 2";

2° dans le paragraphe 1, un alinéa rédigé comme suit est inséré entre les alinéas 1 et 2:

"Les acteurs suivants sont tenus de collaborer conformément à l'alinéa précédent:

— l'opérateur d'un réseau de communications électroniques; et

— toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.";

3° le paragraphe 2 est remplacé par ce qui suit:

"§ 2. Les acteurs visés au § 1er, alinéa 2, communiquent les renseignements requis en temps réel ou, le cas échéant, au moment précisé dans la décision, selon les modalités fixées par l'arrêté royal pris en exécution de l'article 88*bis*, § 2, alinéas 1er et 3.

Toute personne qui refuse de prêter son concours technique aux réquisitions visées dans le présent article ou ne le prête pas en temps réel ou, le cas échéant, au moment précisé dans la décision est punie d'une amende de vingt-six euros à dix mille euros.".

TITRE 3

Dispositions modifiant le Code pénal

Article 29

Dans le Code pénal, l'intitulé du Livre 2, Titre IV, Chapitre V*bis* est remplacé par ce qui suit:

"Boek 2, Titel IV, Hoofdstuk Vbis – Onderscheppen, kennisnemen en opnemen van niet voor het publiek toegankelijke communicatie en gegevens van een informaticasysteem".

Artikel 30

In artikel 259*bis* van hetzelfde wetboek, ingevoegd bij de wet van 30 juni 2004, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1 wordt de bepaling onder 1° vervangen als volgt:

"1° ofwel, opzettelijk, met behulp van enig toestel niet voor publiek toegankelijke communicatie, waaraan hij niet deelneemt, onderschept of doet onderscheppen, er kennis van neemt of doet van nemen, opneemt of doet opnemen, zonder de toestemming van alle deelnemers aan die communicatie";

2° in paragraaf 1 wordt de bepaling onder 3° vervangen als volgt:

"3° ofwel, wetens, de inhoud van niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem die onwettig onderschept of opgenomen zijn of waarvan onwettig kennis genomen is, onder zich houdt, aan een andere persoon onthult of verspreidt, of wetens enig gebruik maakt van een op die manier verkregen inlichting.";

3° in paragraaf 2 worden de woorden "een wettig gemaakte opname van privécommunicatie of –telecommunicatie" vervangen door de woorden "een wettig gemaakte opname van niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem.".

Artikel 31

In hetzelfde wetboek wordt het opschrift van Boek 2, Titel V, Hoofdstuk VIII*bis* vervangen als volgt:

"Boek 2, Titel V, Hoofdstuk VIII*bis* – Misdrijven betreffende het geheim van niet voor het publiek toegankelijke communicatie en gegevens van een informaticasysteem".

Artikel 32

In artikel 314*bis* van hetzelfde wetboek worden de volgende wijzigingen aangebracht:

"Interception, prise de connaissance et enregistrement de communications non accessibles au public et de données d'un système informatique".

Article 30

A l'article 259*bis* du même Code, inséré par la loi de 30 juin 2004, les modifications suivantes sont apportées:

1°dans le paragraphe 1, le 1° est remplacé par ce qui suit:

"1° soit, intentionnellement, à l'aide d'un appareil quelconque, intercepte ou fait intercepter, prend connaissance ou fait prendre connaissance, enregistre ou fait enregistrer des communications non accessibles au public, auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications";

2° dans le paragraphe 1, le 3° est remplacé par ce qui suit:

"3° soit, sciemment, détient, révèle ou divulgue à une autre personne le contenu de communications non accessibles au public ou de données d'un système informatique illégalement interceptées ou enregistrées, ou dont il a pris connaissance illégalement, ou utilise sciemment d'une manière quelconque une information obtenue de cette façon.";

3° dans le paragraphe 2 les mots "de communications ou de télécommunications privées" sont remplacés par les mots "de communications non accessibles au public ou de données d'un système informatique.".

Article 31

Dans le même code, l'intitulé du Livre 2, Titre V, Chapitre VII*bis* est remplacé par ce qui suit:

"Livre 2, Titre V, Chapitre VIII*bis* – Infractions relatives au secret des communications non accessibles au public et des données d'un système informatique".

Article 32

A l'article 314*bis* du même Code, les modifications suivantes sont apportées:

1° in paragraaf 1 wordt de bepaling onder 1° vervangen als volgt:

"1° ofwel, opzettelijk, met behulp van enig toestel niet voor publiek toegankelijke communicatie, waaraan hij niet deelneemt, onderschept of doet onderscheppen, er kennis van neemt of doet van nemen, opneemt of doet opnemen, zonder de toestemming van alle deelnemers aan die communicatie;";

2° paragraaf 2 wordt vervangen als volgt:

"§ 2. Met gevangenisstraf van zes maanden tot twee jaar en met geldboete van vijfhonderd [euro] tot twintigduizend [euro] of met een van die straffen alleen wordt gestraft hij, die wetens, de inhoud van niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem die onwettig onderschept of opgenomen zijn of waarvan onwettig kennis genomen is, onder zich houdt, aan een andere persoon onthult of verspreidt, of wetens enig gebruik maakt van een op die manier verkregen inlichting.

Met dezelfde straffen wordt gestraft hij die, met bedrieglijk opzet of met het oogmerk te schaden, gebruik maakt van een wettig gemaakte opname van niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem.".

TITEL 4

Bepaling tot de oprichting van een gegevensbank stemafdrukken

Artikel 33

De technische gegevens die het mogelijk maken de stem te herkennen van de personen, die het voorwerp uitmaken of hebben uitgemaakt van een maatregel tot interceptie bedoeld in artikel 90*ter*, § 1, van het Wetboek van Strafvordering en die bedoeld worden in artikel 44/5, § 3, 1° van de wet van 5 augustus 1992 op het politieambt, worden gedurende ten hoogste 10 jaar bewaard in de Algemene Nationale Gegevensbank bedoeld in dezelfde wet, met het oog op de identificatie van die personen in het kader van afluisterdossiers uitgevoerd op verzoek van de gerechtelijke overheden.

Behalve die technische gegevens bevat deze gegevensbank ook de gegevens over het dossiernummer, de bevoegde magistraat en het bedoelde gerechtelijke arrondissement.

1° dans le paragraphe 1, le 1° est remplacé par ce qui suit:

"1° soit, intentionnellement, à l'aide d'un appareil quelconque, intercepte ou fait intercepter, prend connaissance ou fait prendre connaissance, enregistre ou fait enregistrer des communications non accessibles au public, auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications;";

2° le paragraphe 2 est remplacé par ce qui suit:

"§ 2. Sera puni d'un emprisonnement de six mois à deux ans et d'une amende de cinq cents [euros] à vingt mille [euros] ou d'une de ces peines seulement, quiconque détient, révèle ou divulgue sciemment à une autre personne le contenu de communications non accessibles au public et de données d'un système informatique illégalement interceptées ou enregistrées, ou dont il a pris connaissance illégalement, ou utilise sciemment d'une manière quelconque une information obtenue de cette façon.

Sera puni des mêmes peines quiconque, avec une intention frauduleuse ou à dessein de nuire, utilise un enregistrement, légalement effectué, de communications non accessibles au public ou de données d'un système informatique.".

TITRE 4

Disposition pour la création d'une banque de données des empreintes vocales

Article 33

Les données techniques permettant la reconnaissance vocale des personnes, faisant ou ayant fait l'objet d'une mesure d'interception des télécommunications visée à l'article 90*ter*, § 1er du Code d'instruction criminelle et qui sont visées à l'article 44/5, § 3, 1° de la loi de 5 août 1992 sur la fonction de police, sont conservées pendant 10 ans au maximum dans la Banque de données Nationale Générale visée dans la même loi, en vue d'aider à identifier ces personnes dans le cadre de dossiers d'écoute réalisés à la demande des autorités judiciaires.

Outre ces données techniques, cette banque de données contient également les données relatives au numéro de dossier, au magistrat compétent et à l'arrondissement judiciaire visé.

De in het eerste lid bedoelde technische gegevens verschillen van de opnames die worden gemaakt in het kader van de tenuitvoerlegging van de maatregel bedoeld in artikel 90*ter* van het Wetboek van Strafvordering. Die opnames worden niet beoogd door dit artikel.

De doeleinden en nadere regels voor de verwerking van die gegevens worden bepaald in de artikelen 44/7 tot 44/11/1 van de wet van 5 augustus 1992 op het politieambt.

Gegeven te Brussel, 6 juli 2016

FILIP

VAN KONINGSWEGE:

De minister van Justitie,

Koen GEENS

Les données techniques visées au premier alinéa sont distinctes des enregistrements réalisés dans le cadre de la mise en œuvre de la mesure visée à l'article 90*ter*, § 1er du Code d'instruction criminelle. Ces enregistrements ne sont pas concernés par le présent article.

Les finalités et les modalités de traitement de ces données sont celles prévues aux articles 44/7 à 44/11/1 de la loi de 5 août 1992 sur la fonction de police.

Donné à Bruxelles, le 6 juillet 2016

PHILIPPE

PAR LE ROI:

Le ministre de la Justice,

Koen GEENS

BIJLAGE

ANNEXE

	Voorontwerp van wet betreffende de verbetering van de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden
WETBOEK STRAFVORDERING	**WETBOEK STRAFVORDERING**
Artikel 39bis	**Artikel 39bis**
§ 1. Onverminderd de specifieke bepalingen van dit artikel, zijn de regels van dit wetboek inzake inbeslagneming, met inbegrip van artikel 28sexies, van toepassing op het kopiëren, ontoegankelijk maken en verwijderen van in een informaticasysteem opgeslagen gegevens.	§ 1. Onverminderd de specifieke bepalingen van dit artikel, zijn de regels van dit wetboek inzake inbeslagneming, met inbegrip van artikel 28sexies, van toepassing op het kopiëren, ontoegankelijk maken en verwijderen van in een informaticasysteem **<u>of een deel ervan</u>** opgeslagen gegevens. § 2. **<u>Tot de zoeking in een informaticasysteem of een deel ervan dat in beslag genomen is, kan beslist worden door een officier van gerechtelijke politie.</u>** **<u>Onverminderd het vorige lid, kan de procureur des Konings een zoeking bevelen in een informaticasysteem of een deel ervan dat door hem in beslag kan worden genomen.</u>** **<u>De zoekingen bedoeld in het eerste en het tweede lid kunnen zich enkel uitstrekken tot de gegevens die opgeslagen zijn op het informaticasysteem dat, respectievelijk, in beslag genomen is of in beslag kan worden genomen.</u>**
§ 2. Wanneer de procureur des Konings of de arbeidsauditeur in een informaticasysteem opgeslagen gegevens aantreft die nuttig zijn voor dezelfde doeleinden als de inbeslagneming, maar de inbeslagneming van de drager daarvan evenwel niet wenselijk is, worden deze gegevens, evenals de gegevens noodzakelijk om deze te kunnen verstaan, gekopieerd op dragers, die toebehoren aan de overheid. In geval van dringendheid of om technische redenen, kan gebruik gemaakt worden van dragers, die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken.	(cf. §6, lid 1)
§ 3. Hij wendt bovendien de passende technische middelen aan om de toegang	(cf. §6, lid 2)

totdeze gegevens in het informaticasysteem, evenals tot de kopieën daarvan die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken, te verhinderen en hun integriteit te waarborgen.	
Indien de gegevens het voorwerp van het misdrijf vormen of voortgekomen zijn uit het misdrijf en indien de gegevens strijdig zijn met de openbare orde of de goede zeden, of een gevaar opleveren voor de integriteit van informaticasystemen of gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen, wendt de procureur des Konings of de arbeidsauditeur alle passende technische middelen aan om deze gegevens ontoegankelijk te maken.	(cf. §6, lid 4)
Hij kan evenwel, behoudens in het geval bedoeld in het vorige lid, het verdere gebruik van het geheel of een deel van deze gegevens toestaan, wanneer dit geen gevaar voor de strafvordering oplevert.	(cf. §6, lid 5)
§ 4. Wanneer de in § 2 vermelde maatregel niet mogelijk is om technische redenen of wegens de omvang van de gegevens, wendt hij de passende technische middelen aan om de toegang tot deze gegevens in het informaticasysteem, evenals tot de kopieën daarvan die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken, te verhinderen en hun integriteit te waarborgen.	(cf. §6, lid 3)
(Artikel 88ter) § 1. Wanneer de onderzoeksrechter een zoeking beveelt in een informaticasysteem of een deel daarvan, kan deze zoeking worden uitgebreid naar een informaticasysteem of een deel daarvan dat zich op een andere plaats bevindt dan daar waar de zoeking plaatsvindt: - indien deze uitbreiding noodzakelijk is om de waarheid aan het licht te brengen ten aanzien van het misdrijf dat het voorwerp uitmaakt van de zoeking; en - indien andere maatregelen disproportioneel zouden zijn, of indien er een risico bestaat dat	§ 3. **De procureur des Konings kan** de zoeking in een informaticasysteem of een deel ervan**, aangevat op grond van §2, uitbreiden** naar een informaticasysteem of een deel daarvan dat zich op een andere plaats bevindt dan daar waar de zoeking plaatsvindt : - indien deze uitbreiding noodzakelijk is om de waarheid aan het licht te brengen ten aanzien van het misdrijf dat het voorwerp uitmaakt van de zoeking; en - indien andere maatregelen disproportioneel zouden zijn, of

zonder deze uitbreiding bewijselementen verloren gaan.	indien er een risico bestaat dat zonder deze uitbreiding bewijselementen verloren gaan.
§ 2. De uitbreiding van de zoeking in een informaticasysteem mag zich niet verder uitstrekken dan tot de informaticasystemen of de delen daarvan waartoe de personen die gerechtigd zijn het onderzochte informaticasysteem te gebruiken, in het bijzonder toegang hebben.	De uitbreiding van de zoeking in een informaticasysteem mag zich niet verder uitstrekken dan tot de informaticasystemen of de delen daarvan waartoe de personen die gerechtigd zijn het onderzochte informaticasysteem te gebruiken, in het bijzonder toegang hebben.
§ 3. Inzake de door uitbreiding van de zoeking in een informaticasysteem aangetroffen gegevens, die nuttig zijn voor dezelfde doeleinden als de inbeslagneming, wordt gehandeld zoals bepaald in artikel 39bis. De onderzoeksrechter brengt de verantwoordelijke van dit informaticasysteem op de hoogte, tenzij diens identiteit of woonplaats redelijkerwijze niet achterhaald kan worden.	Inzake de door uitbreiding van de zoeking in een informaticasysteem aangetroffen gegevens, die nuttig zijn voor dezelfde doeleinden als de inbeslagneming, wordt gehandeld zoals bepaald in **§ 6.**
Wanneer blijkt dat deze gegevens zich niet op het grondgebied van het Rijk bevinden, worden ze enkel gekopieerd. In dat geval deelt de onderzoeksrechter dit, via het openbaar ministerie, onverwijld mee aan het ministerie van Justitie, dat de bevoegde overheid van de betrokken Staat hiervan op de hoogte brengt, indien deze redelijkerwijze kan worden bepaald.	Wanneer blijkt dat deze gegevens zich niet op het grondgebied van het Rijk bevinden, worden ze enkel gekopieerd. In dat geval deelt **de procureur des Konings** dit onverwijld mee aan de **Federale Overheidsdienst** Justitie, dat de bevoegde overheid van de betrokken Staat hiervan op de hoogte brengt, indien deze redelijkerwijze kan worden bepaald.
§ 4. Artikel 89bis is van toepassing op de uitbreiding van de zoeking in een informaticasysteem.	**In geval van uiterst dringende noodzakelijkheid of in geval van heterdaad kan de procureur des Konings de uitbreiding van de zoeking bedoeld in het eerste lid mondeling bevelen. Dit bevel wordt zo spoedig mogelijk schriftelijk bevestigd, met vermelding van de heterdaadsituatie of van de redenen van de uiterst dringende noodzakelijkheid.** § 4. **Enkel de onderzoeksrechter kan een andere zoeking bevelen in een informaticasysteem of een deel ervan dan de zoekingen voorzien in de paragrafen 2 en 3:** - **indien deze zoeking noodzakelijk is om de waarheid aan het licht te brengen ten aanzien van het misdrijf dat het voorwerp uitmaakt van de zoeking; en**

	- **indien andere maatregelen disproportioneel zouden zijn, of indien er een risico bestaat dat zonder deze zoeking bewijselementen verloren gaan.** **In geval van uiterst dringende noodzakelijkheid kan de onderzoeksrechter de uitbreiding van de zoeking bedoeld in het eerste lid mondeling bevelen. Dit bevel wordt zo spoedig mogelijk schriftelijk bevestigd, met vermelding van de heterdaadsituatie of van de redenen van de uiterst dringende noodzakelijkheid.** § 5. **Teneinde de maatregelen bedoeld in dit artikel mogelijk te maken, kan de procureur des Konings of de onderzoeksrechter bevelen om, te allen tijde, ook zonder de toestemming van hetzij de eigenaar of zijn rechthebbende, hetzij de gebruiker:** **- elke beveiliging van de betrokken informaticasystemen tijdelijk op te heffen, desgevallend met behulp van technische hulpmiddelen, valse signalen, valse sleutels of valse hoedanigheden;** **- technische middelen in de betrokken informaticasystemen aan te brengen teneinde de door dat systeem opgeslagen, verwerkte of doorgestuurde gegevens te ontcijferen en te decoderen**. **Evenwel kan enkel de onderzoeksrechter deze tijdelijke opheffing van de beveiliging of deze aanbrenging van technische middelen bevelen wanneer dit in het bijzonder noodzakelijk is voor de toepassing van paragraaf 3.** (cf. §2) § 6. **Indien in de betrokken informaticasystemen** opgeslagen gegevens **aangetroffen worden** die nuttig zijn voor dezelfde doeleinden als de inbeslagneming, maar de inbeslagneming van de drager daarvan evenwel niet wenselijk is, worden deze gegevens, evenals de gegevens noodzakelijk om deze te kunnen verstaan, gekopieerd op dragers, die toebehoren aan de overheid. In geval van dringendheid of om technische redenen, kan gebruik gemaakt worden van dragers, die ter beschikking staan van personen die

	gerechtigd zijn om het informaticasysteem te gebruiken.
(cf. §3, lid 1)	Bovendien worden passende technische middelen aangewend om de toegang tot deze gegevens in het informaticasysteem, evenals tot de kopieën daarvan die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken, te verhinderen en hun integriteit te waarborgen.
(cf. §4)	Wanneer de in het eerste lid vermelde maatregel niet mogelijk is om technische redenen of wegens de omvang van de gegevens, wendt **de procureur des Konings** de passende technische middelen aan om de toegang tot deze gegevens in het informaticasysteem, evenals tot de kopieën daarvan die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken, te verhinderen en hun integriteit te waarborgen.
(cf. §3, lid 2)	Indien de gegevens het voorwerp van het misdrijf vormen of voortgekomen zijn uit het misdrijf en indien de gegevens strijdig zijn met de openbare orde of de goede zeden, of een gevaar opleveren voor de integriteit van informaticasystemen of gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen, wendt de procureur des Konings alle passende technische middelen aan om deze gegevens ontoegankelijk te maken **of, na hiervan kopie te hebben genomen, te verwijderen**.
(cf. §3, lid 3)	Hij kan evenwel, behoudens in het geval bedoeld in het vorige lid, het verdere gebruik van het geheel of een deel van deze gegevens toestaan, wanneer dit geen gevaar voor de strafvordering oplevert.
	In geval van uiterst dringende noodzakelijkheid en wanneer het kennelijk gaat om een strafbaar feit zoals bedoeld in de artikelen 137, §3, 6°, 140bis of 383bis, § 1 van het Strafwetboek, kan de procureur des Konings mondeling bevelen dat alle passende technische middelen worden aangewend om de gegevens, die het voorwerp van het misdrijf vormen of voortgekomen zijn uit het misdrijf en die strijdig zijn met de openbare orde of de goede zeden,

	ontoegankelijk te maken. Dit bevel wordt zo spoedig mogelijk schriftelijk bevestigd, met vermelding van de redenen van de uiterst dringende noodzakelijkheid.
§ 5. De procureur des Konings of de arbeidsauditeur brengt de verantwoordelijke van het informaticasysteem op de hoogte van de zoeking in het informaticasysteem en deelt hem een samenvatting mee van de gegevens die zijn gekopieerd, ontoegankelijk gemaakt of verwijderd.	**§ 7. Tenzij diens identiteit of woonplaats redelijkerwijze niet achterhaald kan worden, brengt de** procureur des Konings **of de onderzoeksrechter** de verantwoordelijke van het informaticasysteem **zo spoedig mogelijk** op de hoogte van de zoeking in het informaticasysteem **of de uitbreiding ervan**. **Hij** deelt hem **in voorkomend geval** een samenvatting mee van de gegevens die zijn gekopieerd, ontoegankelijk gemaakt of verwijderd.
§ 6. De procureur des Konings of de arbeidsauditeur wendt de passende technische middelen aan om de integriteit en de vertrouwelijkheid van deze gegevens te waarborgen. Gepaste technische middelen worden aangewend voor de bewaring hiervan op de griffie. Hetzelfde geldt, wanneer gegevens die worden opgeslagen, verwerkt of overgedragen in een informaticasysteem, samen met hun drager in beslag worden genomen, overeenkomstig de vorige artikelen.	**§ 8.** De procureur des Konings wendt de passende technische middelen aan om de integriteit en de vertrouwelijkheid van deze gegevens te waarborgen. Gepaste technische middelen worden aangewend voor de bewaring hiervan op de griffie. Hetzelfde geldt, wanneer gegevens die worden opgeslagen, verwerkt of overgedragen in een informaticasysteem, samen met hun drager in beslag worden genomen, overeenkomstig de vorige artikelen.
	Artikel 39ter (nieuw)
	§1. Bij het opsporen van de misdaden en de wanbedrijven en onverminderd de bevoegdheden bedoeld in de artikelen 39bis, 46bis en 88bis van het Wetboek van strafvordering en de artikelen XII.17, XII.18, XII.19 en XII.20 van het Wetboek van Economisch Recht, kan iedere officier van gerechtelijke politie, wanneer er redenen bestaan om aan te nemen dat gegevens die opgeslagen, verwerkt of overgedragen worden door middel van een informaticasysteem bijzonder kwetsbaar zijn voor verlies of voor wijziging, bij een gemotiveerde en schriftelijke beslissing aan een of

	meerdere natuurlijke personen of rechtspersonen bevelen de gegevens die in hun bezit zijn of waarover zij controle hebben te bewaren. **De gemotiveerde en schriftelijke beslissing vermeldt:** - **de naam en hoedanigheid van de officier van gerechtelijke politie die om de bewaring verzoekt;** - **het strafbare feit waarop het verzoek betrekking heeft;** - **de gegevens die bewaard moeten worden;** - **de duur van bewaring van de gegevens, die niet langer mag zijn dan negentig dagen. Deze termijn kan schriftelijk worden verlengd.** **In spoedeisende gevallen kan de opdracht tot bewaring mondeling worden gegeven. De opdracht moet zo spoedig mogelijk worden bevestigd in de vorm bepaald in het vorige lid.** **§2. De natuurlijke personen of rechtspersonen bedoeld in §1, zorgen ervoor dat de integriteit van de gegevens gewaarborgd is en dat de gegevens op een veilige manier bewaard worden.** **§3. Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.** **Iedere persoon die weigert mee te werken, of die de bewaarde gegevens doet verdwijnen, vernietigt of wijzigt, wordt gestraft met een gevangenisstraf van zes maanden tot een jaar en met een geldboete van 26 tot 20.000 euro of met één van die straffen alleen.**
	Artikel 39quater (nieuw)
	§1. Onverminderd de mogelijkheden tot rechtstreekse samenwerking met buitenlandse operatoren van elektronische communicatienetwerken en

	verstrekkers van elektronische communicatiediensten, kan de procureur des Konings, via de door de Minister van Justitie aangewezen politiedienst , aan een buitenlandse bevoegde autoriteit verzoeken de snelle bewaring te bevelen of op andere wijze op te leggen van gegevens die opgeslagen, verwerkt of overgedragen worden door middel van een informaticasysteem dat zich bevindt op het grondgebied van die bevoegde autoriteit en ten aanzien waarvan een Belgische bevoegde gerechtelijke autoriteit voornemens is een verzoek om rechtshulp in te dienen. **Het verzoek om bewaring is schriftelijk en vermeldt:** - **de naam en hoedanigheid van de autoriteit die om de bewaring verzoekt;** - **het strafbare feit waarop het verzoek betrekking heeft en een korte uiteenzetting van de daarop betrekking hebbende feiten;** - **de gegevens die bewaard moeten worden en het verband met het strafbare feit;** - **alle beschikbare informatie met betrekking tot de bewaarder van de gegevens of de locatie van het informaticasysteem;** - **de noodzaak van de bewaring;** - **het feit dat een verzoek om rechtshulp ingediend zal worden met betrekking tot de bewaarde gegevens;** - **in voorkomend geval, het feit dat de gegevens die bewaard moeten worden verwijzen naar een andere staat dan de staat van de bevoegde buitenlandse autoriteit.** **§2. Indien een internationaal rechtsinstrument tussen België en een andere Staat hierin voorziet, kan een bevoegde autoriteit van die Staat aan de door de Koning aangewezen politiedienst**

	verzoeken de snelle bewaring te bevelen of op andere wijze op te leggen van gegevens die zich bevinden op het Belgische grondgebied en ten aanzien waarvan deze buitenlandse autoriteit voornemens is een verzoek om rechtshulp in te dienen. **Het verzoek om bewaring is schriftelijk en vermeldt:** - **de naam en hoedanigheid van de autoriteit die om de bewaring verzoekt;** - **het strafbare feit waarop het verzoek betrekking heeft en een korte uiteenzetting van de daarop betrekking hebbende feiten;** - **de gegevens die bewaard moeten worden en het verband met het strafbare feit;** - **alle beschikbare informatie met betrekking tot de bewaarder van de gegevens of de locatie van het informaticasysteem;** - **de noodzaak van de bewaring, en** - **het feit dat een verzoek om rechtshulp ingediend zal worden met betrekking tot de bewaarde gegevens;** - **in voorkomend geval, het feit dat de gegevens die bewaard moeten worden verwijzen naar een andere staat dan de staat van de bevoegde buitenlandse autoriteit.** **Na ontvangst van het verzoek bedoeld in het vorige lid, brengt de in het eerste lid bedoelde politiedienst de bevoegde procureur des Konings of onderzoeksrechter daarvan op de hoogte, en neemt zij alle passende maatregelen om onverwijld over te gaan tot de snelle bewaring van de nader omschreven gegevens, overeenkomstig artikel 39ter.** **Onverminderd de internationale rechtsinstrumenten met betrekking tot rechtshulp waardoor België gebonden is**

	en die ertoe strekken deze samenwerking te bevorderen, kan een verzoek om bewaring door de bevoegde procureur des Konings of onderzoeksrechter alleen worden geweigerd indien: - **het verzoek betrekking heeft op een misdrijf dat door België wordt beschouwd als politiek misdrijf of als een met een politiek misdrijf samenhangend feit, of** - **de uitvoering van het verzoek zou kunnen leiden tot aantasting van de soevereiniteit, veiligheid, openbare orde of andere wezenlijke belangen van België.** **Wanneer de in het eerste lid bedoelde politiedienst van mening is dat de gewone bewaring de toekomstige beschikbaarheid van de gegevens niet waarborgt of de vertrouwelijkheid van het onderzoek van de bevoegde buitenlandse autoriteit in gevaar brengt of dit anderszins schaadt, brengt zij de bevoegde buitenlandse autoriteit hiervan onverwijld op de hoogte, die vervolgens bepaalt of het verzoek niettemin moet worden uitgevoerd.** **Een in antwoord op het in het eerste lid bedoelde verzoek verrichte bewaring is voor een periode van ten minste 60 dagen geldig, teneinde de bevoegde buitenlandse autoriteit de mogelijkheid te bieden een verzoek om rechtshulp in te dienen. Na de ontvangst van een dergelijk verzoek blijven de gegevens bewaard in afwachting van een beslissing inzake het verzoek.** **Indien de gegevens die opgeslagen, verwerkt of overgedragen worden door middel van een informaticasysteem verwijzen naar een andere staat dan de staat van de verzoekende bevoegde buitenlandse autoriteit, brengt de in het eerste lid bedoelde politiedienst de bevoegde procureur des Konings of onderzoeksrechter daarvan op de hoogte. Deze gaat zo snel mogelijk over tot de onthulling aan de bevoegde buitenlandse autoriteit van een hoeveelheid identificatiegegevens of oproepgegevens**

	voldoende om te achterhalen wie die operator van het elektronische communicatienetwerk of de verstrekker van de elektronische communicatiedienst is en langs welke weg de communicatie was verzonden.
Artikel 46bis	**Artikel 46bis**
§ 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 overgaan of doen overgaan op basis van ieder gegeven in zijn bezit of door middel van een toegang tot de klantenbestanden van **de actoren bedoeld in het tweede lid, eerste en tweede streepje,** 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 **dienst zoals bedoeld in het tweede lid, tweede streepje,** of van het gebruikte elektronische communicatiemiddel;
2° de identificatie van de elektronische communicatiediensten waarop een bepaald persoon geabonneerd is of die door een bepaald persoon gewoonlijk gebruikt worden.	2° de identificatie van de **diensten zoals bedoeld in het tweede lid, tweede streepje,** waarop een bepaald persoon geabonneerd is of die door een bepaald persoon gewoonlijk gebruikt worden. **Hiertoe kan hij zo nodig, rechtstreeks of via de door de Koning aangewezen politiedienst, de medewerking vorderen van:** **- de operator van een elektronisch communicatienetwerk; en** **- iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder wordt ook de**

	verstrekker van een elektronische communicatiedienst begrepen.
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 uiterst dringende noodzakelijkheid.	In geval van uiterst dringende noodzakelijkheid **kan de procureur des Konings de maatregel mondeling bevelen**. **De beslissing wordt zo spoedig mogelijk schriftelijk bevestigd**. 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.
§ 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. **De actoren bedoeld in § 1, tweede lid, eerste en tweede streepje,** van wie gevorderd wordt de in paragraaf 1 bedoelde gegevens mee te delen, **verstrekken** de procureur des Konings of de officier van gerechtelijke politie de gegevens die werden opgevraagd **in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, volgens de modaliteiten vastgesteld** 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.	**<u>Iedere persoon die de gegevens weigert mee te delen of niet meedeelt in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering,</u>** wordt gestraft met geldboete van zesentwintig euro tot tienduizend euro.
Artikel 46quinquies	**Artikel 46quinquies**
§ 1. Onverminderd artikel 89ter, kan de procureur des Konings bij een schriftelijke en met redenen omklede beslissing de politiediensten machtigen om te allen tijde, buiten medeweten van de eigenaar of van zijn rechthebbende, of zonder hun toestemming, een private plaats te betreden, wanneer er ernstige aanwijzingen zijn dat de strafbare feiten een misdrijf uitmaken of zouden uitmaken als bedoeld in artikel 90ter, §§ 2 tot 4, of gepleegd worden of zouden worden in het kader van een criminele organisatie zoals bedoeld in artikel 324bis van het Strafwetboek, en de overige middelen van onderzoek niet lijken te volstaan om de waarheid aan de dag te brengen. Een private plaats in de zin van dit artikel is de plaats die kennelijk: - geen woning is; - geen door een woning omsloten eigen aanhorigheid in de zin van de artikelen 479, 480 en 481 van het Strafwetboek is; - geen lokaal aangewend voor beroepsdoeleinden of de woonplaats van een advocaat of een arts is als bedoeld in artikel 56bis, derde lid. In spoedeisende gevallen kan de in het eerste lid bedoelde beslissing mondeling worden meegedeeld. De beslissing moet in dat geval zo spoedig mogelijk schriftelijk met redenen omkleed en bevestigd worden. Ingeval de in het eerste lid bedoelde beslissing genomen wordt in het kader van de toepassing van de bijzondere opsporingsmethoden zoals bedoeld in de artikelen 47ter tot 47decies, worden de beslissing en alle ermee verband houdende processen-verbaal uiterlijk na	§ 1. Onverminderd artikel 89ter, kan de procureur des Konings bij een schriftelijke en met redenen omklede beslissing de politiediensten machtigen om te allen tijde, buiten medeweten van de eigenaar of van zijn rechthebbende, of zonder hun toestemming, een private plaats te betreden **<u>en gesloten voorwerpen die zich op deze plaats bevinden te openen</u>**, wanneer er ernstige aanwijzingen zijn dat de strafbare feiten een misdrijf uitmaken of zouden uitmaken als bedoeld in artikel 90ter, §§ 2 tot 4, of gepleegd worden of zouden worden in het kader van een criminele organisatie zoals bedoeld in artikel 324bis van het Strafwetboek, en de overige middelen van onderzoek niet lijken te volstaan om de waarheid aan de dag te brengen. Een private plaats in de zin van dit artikel is de plaats die kennelijk : - geen woning is; - geen door een woning omsloten eigen aanhorigheid in de zin van de artikelen 479, 480 en 481 van het Strafwetboek is; - geen lokaal aangewend voor beroepsdoeleinden of de woonplaats van een advocaat of een arts is als bedoeld in artikel 56bis, derde lid. In spoedeisende gevallen kan de in het eerste lid bedoelde beslissing mondeling worden meegedeeld. De beslissing moet in dat geval zo spoedig mogelijk schriftelijk met redenen omkleed en bevestigd worden. Ingeval de in het eerste lid bedoelde beslissing genomen wordt in het kader van de toepassing van de bijzondere opsporingsmethoden zoals bedoeld in de artikelen 47ter tot 47decies, worden de beslissing en alle ermee verband houdende

het beëindigen van de bijzondere opsporingsmethode bij het strafdossier gevoegd.	processen-verbaal uiterlijk na het beëindigen van de bijzondere opsporingsmethode bij het strafdossier gevoegd.
§ 2. Het betreden van de private plaats zoals bedoeld in § 1 kan enkel geschieden teneinde:	§ 2. Het **betreden van de private plaats zoals bedoeld in §1, en het openen van gesloten voorwerpen die zich op deze plaats bevinden** kan enkel geschieden teneinde :
1° die plaats op te nemen en zich te vergewissen van de eventuele aanwezigheid van zaken die het voorwerp van het misdrijf uitmaken, die gediend hebben of bestemd zijn tot het plegen ervan of die uit een misdrijf voortkomen, van de vermogensvoordelen die rechtstreeks uit het misdrijf zijn verkregen, van de goederen en waarden die in de plaats ervan zijn gesteld of van de inkomsten uit de belegde voordelen;	1° die plaats op te nemen en zich te vergewissen van de eventuele aanwezigheid van zaken die het voorwerp van het misdrijf uitmaken, die gediend hebben of bestemd zijn tot het plegen ervan of die uit een misdrijf voortkomen, van de vermogensvoordelen die rechtstreeks uit het misdrijf zijn verkregen, van de goederen en waarden die in de plaats ervan zijn gesteld of van de inkomsten uit de belegde voordelen;
2° de bewijzen te verzamelen van de aanwezigheid van de zaken bedoeld in 1°;	2° de bewijzen te verzamelen van de aanwezigheid van de zaken bedoeld in 1°;
3° in het kader van een observatie een technisch hulpmiddel als bedoeld in artikel 47sexies, § 1, derde lid, te plaatsen.	3° in het kader van een observatie een technisch hulpmiddel als bedoeld in artikel 47sexies, § 1, derde lid, te plaatsen**, te herstellen of terug te nemen**;
	4° de overeenkomstig § 5 meegenomen voorwerpen terug te plaatsen.
§ 3. Een inkijkoperatie kan door de procureur des Konings enkel worden beslist ten aanzien van plaatsen waarvan men op basis van precieze aanwijzingen vermoedt dat de zaken bedoeld in § 2, 1°, er zich bevinden, dat er bewijzen van kunnen verzameld worden, of dat ze gebruikt worden door personen op wie een verdenking rust.	§ 3. Een inkijkoperatie kan door de procureur des Konings enkel worden beslist ten aanzien van plaatsen waarvan men op basis van precieze aanwijzingen vermoedt dat de zaken bedoeld in § 2, 1°, er zich bevinden, dat er bewijzen van kunnen verzameld worden, of dat ze gebruikt worden door personen op wie een verdenking rust.
§ 4. Het aanwenden van technische hulpmiddelen met het in § 2 beoogde doel, wordt gelijkgesteld met het betreden van een private plaats zoals bepaald in § 1.	§ 4. Het aanwenden van technische hulpmiddelen met het in § 2 beoogde doel, wordt gelijkgesteld met het betreden van een private plaats zoals bepaald in § 1.
	§ 5. Indien het onderzoek van een in § 1 bedoeld voorwerp niet ter plaatse kan gebeuren en indien de informatie niet op een andere manier kan worden verkregen, is het de politiedienst toegestaan dit

	voorwerp mee te nemen voor een strikt beperkte duur. Het bewuste voorwerp wordt zo spoedig mogelijk teruggeplaatst, tenzij dit het goede verloop van het onderzoek in de weg staat. **§ 6. In het kader van de maatregel bedoeld in §1, is het binnendringen in een informaticasysteem enkel mogelijk met het oog op de doeleinden bedoeld in §2, 3°.** **§ 7. De officier van gerechtelijke politie die de leiding heeft over de uitvoering van de maatregel bedoeld in § 1 of in artikel 89ter, § 1, stelt van het verloop van de maatregel een proces-verbaal op. Wanneer tijdens de uitvoering van de maatregel gesloten voorwerpen geopend werden of toepassing gemaakt werd van §5, wordt daarvan melding gemaakt in het proces-verbaal. Het proces-verbaal wordt uiterlijk na het beëindigen van de maatregel bij het strafdossier gevoegd.**
	Artikel 46sexies (nieuw)
	§ 1. Bij het opsporen van de misdaden en de wanbedrijven, wanneer het onderzoek zulks vereist en de overige middelen van onderzoek niet lijken te volstaan om de waarheid aan de dag te brengen, kan de procureur des Konings de politiediensten bedoeld in het tweede lid machtigen om op het internet, desgevallend onder een fictieve identiteit, contact te onderhouden met een of meerdere personen waarvan er ernstige aanwijzingen zijn dat zij strafbare feiten die een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben, plegen of zouden plegen. **De Koning bepaalt de voorwaarden, onder meer voor wat de opleiding betreft, en de modaliteiten voor de aanwijzing van de politiediensten die bevoegd zijn om de maatregel, bedoeld in dit artikel, ten uitvoer te leggen.** **In uitzonderlijke omstandigheden en mits**

	uitdrukkelijke machtiging van de procureur des Konings, kan de in het eerste lid bedoelde politieambtenaar bij een welbepaalde operatie kortstondig een beroep doen op de deskundigheid van een persoon die niet tot de politiediensten behoort, indien dit strikt noodzakelijk voorkomt voor het welslagen van zijn opdracht. **Dit artikel is niet van toepassing op de persoonlijke interactie op het internet van politieambtenaren, bij de uitvoering van hun opdrachten van gerechtelijke politie, met een of meerdere personen, die enkel een gerichte verificatie of een arrestatie tot direct doel heeft, en dit zonder gebruik te maken van een geloofwaardige fictieve identiteit.** **§ 2. De maatregel bedoeld in § 1 wordt door de procureur des Konings bevolen met een voorafgaandelijke en met redenen omklede schriftelijke machtiging. Deze machtiging is geldig voor een termijn van drie maanden, onverminderd hernieuwing.** **In spoedeisende gevallen kan de machtiging mondeling worden verstrekt. De machtiging moet zo spoedig mogelijk worden bevestigd in de vorm bepaald in het eerste lid.** **§ 3. Blijven vrij van straf de politieambtenaren die, in het kader van hun opdracht en met het oog op het welslagen ervan of ter verzekering van hun eigen veiligheid of deze van andere bij de maatregel betrokken personen, strikt noodzakelijke strafbare feiten plegen, mits uitdrukkelijk akkoord van de procureur des Konings.** **Die strafbare feiten mogen niet ernstiger zijn dan die waarvoor de maatregel wordt aangewend en moeten noodzakelijkerwijze evenredig zijn met het nagestreefde doel.** **Het eerste en het tweede lid zijn eveneens van toepassing op de personen die aan de uitvoering van deze opdracht noodzakelijke en rechtstreekse hulp of bijstand hebben verleend en op de**

	personen, bedoeld in § 1, derde lid. **Blijft vrij van straf de magistraat die, met inachtneming van dit wetboek, machtiging verleent aan een politieambtenaar en aan de personen bedoeld in het derde lid tot het plegen van strafbare feiten in het kader van de uitvoering van de maatregel.** **De politieambtenaren melden schriftelijk en vóór de uitvoering van de maatregel aan de procureur des Konings, de misdrijven die zij of de personen bedoeld in het derde lid, voornemens zijn te plegen.** **Indien deze voorafgaande kennisgeving niet kon gebeuren, stellen de politieambtenaren de procureur des Konings onverwijld in kennis van de misdrijven die zij of de personen bedoeld in het derde lid, hebben gepleegd en bevestigen dit nadien schriftelijk.** **De procureur des Konings vermeldt in een afzonderlijke en schriftelijke beslissing de misdrijven die door de politiediensten en de personen bedoeld in het derde lid in het kader van deze door hem bevolen maatregel kunnen worden gepleegd. Deze beslissing wordt in een afzonderlijk en vertrouwelijk dossier bewaard. Hij heeft als enige toegang tot dit dossier, onverminderd het in artikel 56bis, respectievelijk de artikelen 235ter, § 3 en 235quater, § 3 bedoelde inzagerecht van de onderzoeksrechter en de kamer van inbeschuldigingstelling. De inhoud van dit dossier valt onder het beroepsgeheim.** **§ 4. De met het onderzoek belaste officier van gerechtelijke politie stelt proces-verbaal op van de verschillende fasen in de uitvoering van deze maatregel, met inbegrip van de relevante contacten. Deze processen-verbaal worden uiterlijk na het beëindigen van de maatregel bij het dossier gevoegd.** **De contacten bedoeld in § 1 worden met de passende technische middelen geregistreerd en uiterlijk na het beëindigen van de maatregel bij het**

	dossier gevoegd of ter griffie, al dan niet in digitale vorm, neergelegd. **§ 5. De procureur des Konings staat in voor de tenuitvoerlegging van de machtigingen tot de maatregel bedoeld in § 1, eerste lid, die zijn verleend door de onderzoeksrechter in het kader van een gerechtelijk onderzoek overeenkomstig artikel 56bis.** **De procureur des Konings vermeldt op dat ogenblik in een afzonderlijke en schriftelijke beslissing de misdrijven die door de politiediensten en de personen bedoeld § 3, derde lid, in het kader van de door de onderzoeksrechter bevolen maatregel kunnen worden gepleegd. Deze beslissing wordt in het dossier bedoeld in § 3, zevende lid, bewaard.**
Artikel 47sexies	**Artikel 47sexies**
§ 1. Observatie in de zin van dit wetboek is het stelselmatig waarnemen door een politieambtenaar van één of meerdere personen, hun aanwezigheid of gedrag, of van bepaalde zaken, plaatsen of gebeurtenissen. Een stelselmatige observatie in de zin van dit wetboek is een observatie van meer dan vijf opeenvolgende dagen of van meer dan vijf niet-opeenvolgende dagen gespreid over een periode van een maand, een observatie waarbij technische hulpmiddelen worden aangewend, een observatie met een internationaal karakter, of een observatie uitgevoerd door de gespecialiseerde eenheden van de federale politie. Een technisch hulpmiddel in de zin van dit wetboek is een configuratie van componenten die signalen detecteert, deze transporteert, hun registratie activeert en de signalen registreert, met uitzondering van de technische middelen die worden aangewend om een maatregel als bedoeld in artikel 90ter uit te voeren. Een toestel gebruikt voor het nemen van foto's wordt uitsluitend beschouwd als een technisch hulpmiddel in de zin van dit	§ 1. Observatie in de zin van dit wetboek is het stelselmatig waarnemen door een politieambtenaar van één of meerdere personen, hun aanwezigheid of gedrag, of van bepaalde zaken, plaatsen of gebeurtenissen. Een stelselmatige observatie in de zin van dit wetboek is een observatie van meer dan vijf opeenvolgende dagen of van meer dan vijf niet-opeenvolgende dagen gespreid over een periode van een maand, een observatie waarbij technische hulpmiddelen worden aangewend, een observatie met een internationaal karakter, of een observatie uitgevoerd door de gespecialiseerde eenheden van de federale politie. Een technisch hulpmiddel in de zin van dit wetboek is een configuratie van componenten die signalen detecteert, deze transporteert, hun registratie activeert en de signalen registreert, met uitzondering van de technische middelen die worden aangewend om een maatregel als bedoeld in artikel 90ter uit te voeren. Een toestel gebruikt voor het nemen van foto's wordt uitsluitend beschouwd als een technisch hulpmiddel in de zin van dit

Wetboek in het geval bedoeld in artikel 56bis, tweede lid.	Wetboek in het geval bedoeld in artikel 56bis, tweede lid.
§ 2. De procureur des Konings kan in het kader van het opsporingsonderzoek een observatie machtigen wanneer het onderzoek zulks vereist en de overige middelen van onderzoek niet lijken te volstaan om de waarheid aan de dag te brengen.	§ 2. De procureur des Konings kan in het kader van het opsporingsonderzoek een observatie machtigen wanneer het onderzoek zulks vereist en de overige middelen van onderzoek niet lijken te volstaan om de waarheid aan de dag te brengen.
Een observatie met gebruik van technische hulpmiddelen kan enkel gemachtigd worden wanneer er ernstige aanwijzingen zijn dat de strafbare feiten een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben.	Een observatie met gebruik van technische hulpmiddelen kan enkel gemachtigd worden wanneer er ernstige aanwijzingen zijn dat de strafbare feiten een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben.
§ 3. De machtiging tot observatie is schriftelijk en vermeldt :	§ 3. De machtiging tot observatie is schriftelijk en vermeldt :
1° de ernstige aanwijzingen van het strafbaar feit die de observatie wettigen en indien de observatie zich situeert in het proactieve onderzoek zoals omschreven in artikel 28bis, § 2, de bijzondere aanwijzingen met betrekking tot de elementen omschreven in deze laatste bepaling;	1° de ernstige aanwijzingen van het strafbaar feit die de observatie wettigen**, of,** indien de observatie zich situeert in het proactieve onderzoek zoals omschreven in artikel 28bis, § 2, **het redelijk vermoeden van te plegen of reeds gepleegde maar nog niet aan het licht gebrachte strafbare feiten, en** de bijzondere aanwijzingen met betrekking tot de elementen omschreven in deze laatste bepaling**, die de observatie wettigen**;
2° de redenen waarom de observatie onontbeerlijk is om de waarheid aan de dag te brengen;	2° de redenen waarom de observatie onontbeerlijk is om de waarheid aan de dag te brengen;
3° de naam of indien die niet bekend is, een zo nauwkeurig mogelijke beschrijving van de geobserveerde persoon of personen, alsmede van de zaken, plaatsen of gebeurtenissen bedoeld in § 1;	3° de naam of indien die niet bekend is, een zo nauwkeurig mogelijke beschrijving van de geobserveerde persoon of personen, alsmede van de zaken, plaatsen of gebeurtenissen bedoeld in § 1;
4° de wijze waarop aan de observatie uitvoering zal worden gegeven, daaronder begrepen de toelating tot het gebruik van technische hulpmiddelen in de gevallen bepaald bij § 2, tweede lid, en artikel 56bis, tweede lid. In dit laatste geval vermeldt de machtiging van de onderzoeksrechter het adres of een zo nauwkeurig mogelijke plaatsbepaling van de woning waarop de observatie betrekking heeft;	4° de wijze waarop aan de observatie uitvoering zal worden gegeven, daaronder begrepen de toelating tot het gebruik van technische hulpmiddelen in de gevallen bepaald bij § 2, tweede lid, en artikel 56bis, tweede lid. In dit laatste geval vermeldt de machtiging van de onderzoeksrechter het adres of een zo nauwkeurig mogelijke plaatsbepaling van de woning waarop de observatie betrekking heeft;
5° de periode tijdens welke de observatie	5° de periode tijdens welke de observatie

kan worden uitgevoerd en die niet langer mag zijn dan één maand te rekenen van de datum van de machtiging;	kan worden uitgevoerd en die niet langer mag zijn dan **drie maanden** te rekenen van de datum van de machtiging;
6° de naam en de hoedanigheid van de officier van gerechtelijke politie, die de leiding heeft over de uitvoering van de observatie.	6° de naam en de hoedanigheid van de officier van gerechtelijke politie, die de leiding heeft over de uitvoering van de observatie.
§ 4. De procureur des Konings vermeldt op dat ogenblik in een afzonderlijke en schriftelijke beslissing de misdrijven die door de politiediensten en de personen bedoeld in artikel 47quinquies, § 2, derde lid, in het kader van de observatie kunnen worden gepleegd.	§ 4. De procureur des Konings vermeldt op dat ogenblik in een afzonderlijke en schriftelijke beslissing de misdrijven die door de politiediensten en de personen bedoeld in artikel 47quinquies, § 2, derde lid, in het kader van de observatie kunnen worden gepleegd.
Deze beslissing wordt in het dossier bedoeld in artikel 47septies, § 1, tweede lid, bewaard.	Deze beslissing wordt in het dossier bedoeld in artikel 47septies, § 1, tweede lid, bewaard.
§ 5. In spoedeisende gevallen kan de machtiging tot observatie mondeling worden verstrekt. De machtiging moet zo spoedig mogelijk worden bevestigd in de vorm bepaald in het eerste lid.	§ 5. In spoedeisende gevallen kan de machtiging tot observatie mondeling worden verstrekt. De machtiging moet zo spoedig mogelijk worden bevestigd in de vorm bepaald in **§3**.
§ 6. De procureur des Konings kan steeds op gemotiveerde wijze zijn machtiging tot observatie wijzigen, aanvullen of verlengen. Hij kan te allen tijde zijn machtiging intrekken. Hij gaat bij elke wijziging, aanvulling of verlenging van zijn machtiging na of de voorwaarden bepaald in §§ 1 tot 3, zijn vervuld en handelt daarbij overeenkomstig § 3, 1° tot 6°.	§ 6. De procureur des Konings kan steeds op gemotiveerde wijze zijn machtiging tot observatie wijzigen, aanvullen of verlengen. Hij kan te allen tijde zijn machtiging intrekken. Hij gaat bij elke wijziging, aanvulling of verlenging van zijn machtiging na of de voorwaarden bepaald in §§ 1 tot 3, zijn vervuld en handelt daarbij overeenkomstig § 3, 1° tot 6°.
§ 7. De procureur des Konings staat in voor de tenuitvoerlegging van de machtigingen tot observatie die zijn verleend door de onderzoeksrechter in het kader van een gerechtelijk onderzoek overeenkomstig artikel 56bis.	§ 7. De procureur des Konings staat in voor de tenuitvoerlegging van de machtigingen tot observatie die zijn verleend door de onderzoeksrechter in het kader van een gerechtelijk onderzoek overeenkomstig artikel 56bis.
De procureur des Konings vermeldt op dat ogenblik in een afzonderlijke en schriftelijke beslissing de misdrijven die door de politiediensten en de personen bedoeld in artikel 47quinquies, § 2, derde lid, in het kader van de door de onderzoeksrechter bevolen observatie kunnen worden gepleegd. Deze beslissing wordt in het dossier bedoeld in artikel 47septies, § 1, tweede lid, bewaard.	De procureur des Konings vermeldt op dat ogenblik in een afzonderlijke en schriftelijke beslissing de misdrijven die door de politiediensten en de personen bedoeld in artikel 47quinquies, § 2, derde lid, in het kader van de door de onderzoeksrechter bevolen observatie kunnen worden gepleegd. Deze beslissing wordt in het dossier bedoeld in artikel 47septies, § 1, tweede lid, bewaard.

Artikel 47octies	**Artikel 47octies**
§ 1. Infiltratie in de zin van dit wetboek is het door een politieambtenaar, infiltrant genoemd, onder een fictieve identiteit, duurzaam contact onderhouden met een of meerdere personen, waarvan er ernstige aanwijzingen zijn dat zij strafbare feiten in het kader van een criminele organisatie, zoals bedoeld in artikel 324bis van het Strafwetboek, of misdaden of wanbedrijven als bedoeld in artikel 90ter, §§ 2 tot 4 plegen of zouden plegen.	§ 1. Infiltratie in de zin van dit wetboek is het door een politieambtenaar, infiltrant genoemd, onder een fictieve identiteit, duurzaam contact onderhouden met een of meerdere personen, waarvan er ernstige aanwijzingen zijn dat zij strafbare feiten in het kader van een criminele organisatie, zoals bedoeld in artikel 324bis van het Strafwetboek, of misdaden of wanbedrijven als bedoeld in artikel 90ter, §§ 2 tot 4 plegen of zouden plegen.
In uitzonderlijke omstandigheden en mits uitdrukkelijke machtiging van de bevoegde magistraat, kan de infiltrant bij een welbepaalde operatie kortstondig een beroep doen op de deskundigheid van een persoon die niet tot de politiediensten behoort, indien dit strikt noodzakelijk voorkomt voor het welslagen van zijn opdracht.	In uitzonderlijke omstandigheden en mits uitdrukkelijke machtiging van de bevoegde magistraat, kan de infiltrant bij een welbepaalde operatie kortstondig een beroep doen op de deskundigheid van een persoon die niet tot de politiediensten behoort, indien dit strikt noodzakelijk voorkomt voor het welslagen van zijn opdracht.
§ 2. De procureur des Konings kan in het kader van het opsporingsonderzoek een infiltratie machtigen wanneer het onderzoek zulks vereist en de overige middelen van onderzoek niet lijken te volstaan om de waarheid aan de dag te brengen.	§ 2. De procureur des Konings kan in het kader van het opsporingsonderzoek een infiltratie machtigen wanneer het onderzoek zulks vereist en de overige middelen van onderzoek niet lijken te volstaan om de waarheid aan de dag te brengen.
Hij kan de politiedienst machtigen om, binnen het wettelijk kader van een infiltratie en met inachtneming van de finaliteit ervan, bepaalde politionele onderzoekstechnieken aan te wenden. De Koning bepaalt bij een in Ministerraad overlegd besluit, op voordracht van de minister van Justitie en na advies van het College van procureurs-generaal, deze politionele onderzoekstechnieken. Deze politionele onderzoekstechnieken kunnen slechts worden aangewend door leden van de directie van de speciale eenheden van de federale politie en, desgevallend, mits bijkomend voorafgaand akkoord van de federale procureur, in samenwerking met buitenlandse speciaal daartoe opgeleide en bevoegde ambtenaren.	Hij kan de politiedienst machtigen om, binnen het wettelijk kader van een infiltratie en met inachtneming van de finaliteit ervan, bepaalde politionele onderzoekstechnieken aan te wenden. De Koning bepaalt bij een in Ministerraad overlegd besluit, op voordracht van de minister van Justitie en na advies van het College van procureurs-generaal, deze politionele onderzoekstechnieken. Deze politionele onderzoekstechnieken kunnen slechts worden aangewend door leden van de directie van de speciale eenheden van de federale politie en, desgevallend, mits bijkomend voorafgaand akkoord van de federale procureur, in samenwerking met buitenlandse speciaal daartoe opgeleide en bevoegde ambtenaren.
De procureur des Konings kan tevens, indien daartoe grond bestaat, toelating verlenen om de noodzakelijke maatregelen te nemen ter vrijwaring van de veiligheid en de fysieke, psychische en morele integriteit van de infiltrant. Deze toelating wordt bewaard in het vertrouwelijk dossier bedoeld in artikel 47novies, § 1, tweede lid.	De procureur des Konings kan tevens, indien daartoe grond bestaat, toelating verlenen om de noodzakelijke maatregelen te nemen ter vrijwaring van de veiligheid en de fysieke, psychische en morele integriteit van de infiltrant. Deze toelating wordt bewaard in het vertrouwelijk dossier bedoeld in artikel 47novies, § 1, tweede lid.

§ 3. De machtiging tot infiltratie is schriftelijk en vermeldt :	§ 3. De machtiging tot infiltratie is schriftelijk en vermeldt :
1° de ernstige aanwijzingen van het strafbaar feit die de infiltratie wettigen;	1° de ernstige aanwijzingen van het strafbaar feit die de infiltratie wettigen **of, indien de infiltratie zich situeert in het proactieve onderzoek zoals omschreven in artikel 28bis, §2, het redelijk vermoeden van te plegen of reeds gepleegde maar nog niet aan het licht gebrachte strafbare feiten, en de bijzondere aanwijzingen met betrekking tot de elementen omschreven in deze laatste bepaling, die de infiltratie wettigen;**
2° de redenen waarom de infiltratie onontbeerlijk is om de waarheid aan de dag te brengen;	2° de redenen waarom de infiltratie onontbeerlijk is om de waarheid aan de dag te brengen;
3° indien bekend, de naam of anders een zo nauwkeurig mogelijke beschrijving van de persoon of personen bedoeld in § 1;	3° indien bekend, de naam of anders een zo nauwkeurig mogelijke beschrijving van de persoon of personen bedoeld in § 1;
4° de wijze waarop aan de infiltratie uitvoering zal worden gegeven, daaronder begrepen de toelating kortstondig een beroep te doen op de deskundigheid van een burger, zoals bepaald in § 1, tweede lid, en de toelating politionele onderzoekstechnieken, zoals bepaald in § 2, tweede lid, aan te wenden;	4° de wijze waarop aan de infiltratie uitvoering zal worden gegeven, daaronder begrepen de toelating kortstondig een beroep te doen op de deskundigheid van een burger, zoals bepaald in § 1, tweede lid, en de toelating politionele onderzoekstechnieken, zoals bepaald in § 2, tweede lid, aan te wenden;
5° de periode tijdens welke de infiltratie kan worden uitgevoerd en die niet langer mag zijn dan drie maanden te rekenen van de datum van de machtiging;	5° de periode tijdens welke de infiltratie kan worden uitgevoerd en die niet langer mag zijn dan drie maanden te rekenen van de datum van de machtiging;
6° de naam en de hoedanigheid van de officier van gerechtelijke politie, die de leiding heeft over de uitvoering van de infiltratie.	6° de naam en de hoedanigheid van de officier van gerechtelijke politie, die de leiding heeft over de uitvoering van de infiltratie.
§ 4. De procureur des Konings vermeldt op dat ogenblik in een afzonderlijke en schriftelijke beslissing de misdrijven die door de politiediensten en de personen bedoeld in artikel 47quinquies, § 2, derde lid, in het kader van de infiltratie kunnen worden gepleegd. Deze beslissing wordt in het dossier bedoeld in artikel 47novies, § 1, tweede lid, bewaard.	§ 4. De procureur des Konings vermeldt op dat ogenblik in een afzonderlijke en schriftelijke beslissing de misdrijven die door de politiediensten en de personen bedoeld in artikel 47quinquies, § 2, derde lid, in het kader van de infiltratie kunnen worden gepleegd. Deze beslissing wordt in het dossier bedoeld in artikel 47novies, § 1, tweede lid, bewaard.
§ 5. In spoedeisende gevallen kan de	§ 5. In spoedeisende gevallen kan de

machtiging tot infiltratie mondeling worden verstrekt. De machtiging moet zo spoedig mogelijk worden bevestigd in de vorm bepaald in het eerste lid.	machtiging tot infiltratie mondeling worden verstrekt. De machtiging moet zo spoedig mogelijk worden bevestigd in de vorm bepaald in **§3**.
§ 6. De procureur des Konings kan steeds op gemotiveerde wijze zijn machtiging tot infiltratie wijzigen, aanvullen of verlengen. Hij kan te allen tijde zijn machtiging intrekken. Hij gaat bij elke wijziging, aanvulling of verlenging van zijn machtiging na of de voorwaarden bepaald in §§ 1 tot 3 zijn vervuld en handelt daarbij overeenkomstig § 3, 1° tot 6°.	§ 6. De procureur des Konings kan steeds op gemotiveerde wijze zijn machtiging tot infiltratie wijzigen, aanvullen of verlengen. Hij kan te allen tijde zijn machtiging intrekken. Hij gaat bij elke wijziging, aanvulling of verlenging van zijn machtiging na of de voorwaarden bepaald in §§ 1 tot 3 zijn vervuld en handelt daarbij overeenkomstig § 3, 1° tot 6°.
§ 7. De procureur des Konings staat in voor de tenuitvoerlegging van de machtigingen tot infiltratie die zijn verleend door de onderzoeksrechter in het kader van een gerechtelijk onderzoek overeenkomstig artikel 56bis.	§ 7. De procureur des Konings staat in voor de tenuitvoerlegging van de machtigingen tot infiltratie die zijn verleend door de onderzoeksrechter in het kader van een gerechtelijk onderzoek overeenkomstig artikel 56bis.
De procureur des Konings vermeldt op dat ogenblik in een afzonderlijke en schriftelijke beslissing de misdrijven die door de politiediensten en de personen bedoeld in artikel 47quinquies, § 2, derde lid, in het kader van de door de onderzoeksrechter bevolen infiltratie kunnen worden gepleegd. Deze beslissing wordt in het dossier bedoeld in artikel 47novies, § 1, tweede lid, bewaard.	De procureur des Konings vermeldt op dat ogenblik in een afzonderlijke en schriftelijke beslissing de misdrijven die door de politiediensten en de personen bedoeld in artikel 47quinquies, § 2, derde lid, in het kader van de door de onderzoeksrechter bevolen infiltratie kunnen worden gepleegd. Deze beslissing wordt in het dossier bedoeld in artikel 47novies, § 1, tweede lid, bewaard.
Artikel 47undecies	**Artikel 47undecies**
Ten minste om de drie maanden zendt de procureur des Konings alle dossiers, waarin hij toepassing heeft gemaakt van de bijzondere opsporingsmethoden observatie en infiltratie en waarin hij besloten heeft niet tot vervolging over te gaan, over aan de procureur-generaal teneinde deze in staat te stellen een controle uit te voeren op de wettigheid van de gebruikte methoden.	Ten minste om de drie maanden zendt de procureur des Konings alle dossiers, waarin hij toepassing heeft gemaakt van de bijzondere opsporingsmethoden observatie en infiltratie en waarin hij besloten heeft niet tot vervolging over te gaan, over aan de procureur-generaal teneinde deze in staat te stellen een controle uit te voeren op de wettigheid van de gebruikte methoden.
De procureur-generaal maakt verslag op van deze controle. Het verslag wordt overgezonden aan het college van procureurs-generaal, dat de globale evaluatie en de statistische gegevens met betrekking tot deze verslagen opneemt in zijn jaarverslag, bedoeld in artikel 143bis, § 7, van het Gerechtelijk Wetboek.	De procureur-generaal maakt verslag op van deze controle. Het verslag wordt overgezonden aan het college van procureurs-generaal, dat de globale evaluatie en de statistische gegevens met betrekking tot deze verslagen opneemt in zijn jaarverslag, bedoeld in artikel 143bis, § 7, van het Gerechtelijk Wetboek.
De federale procureur maakt in zijn	De federale procureur maakt in zijn

jaarverslag, bedoeld in artikel 346, § 2, 2°, van hetzelfde Wetboek, de globale evaluatie en de statistische gegevens bekend van de dossiers waarin hij toepassing heeft gemaakt van de bijzondere opsporingsmethoden observatie en infiltratie en waarin hij besloten heeft niet tot vervolging over te gaan. Het college van procureurs-generaal voert een controle uit over alle dossiers waarin de informantenwerking overeenkomstig artikel 47decies, § 7, werd toegepast. Daartoe wordt door de procureur des Koning via de territoriale bevoegde procureur-generaal, of rechtstreeks door de federale procureur een omstandig verslag aan de voorzitter van het college van procureurs-generaal overgezonden. Dit verslag wordt overgezonden zodra de toepassing van deze bijzondere opsporingsmethode werd beëindigd. Het college van procureurs-generaal maakt verslag op van deze controle en neemt de globale evaluatie en de statistische gegevens daaromtrent op in zijn jaarverslag, bedoeld in artikel 143bis, § 7, van het Gerechtelijk Wetboek.	jaarverslag, bedoeld in artikel 346, § 2, 2°, van hetzelfde Wetboek, de globale evaluatie en de statistische gegevens bekend van de dossiers waarin hij toepassing heeft gemaakt van de bijzondere opsporingsmethoden observatie en infiltratie en waarin hij besloten heeft niet tot vervolging over te gaan.
Artikel 56bis	**Artikel 56bis**
In afwijking van artikel 56, § 1, derde lid, worden de machtigingen van de onderzoeksrechter waarbij hij bijzondere opsporingsmethoden beveelt ten uitvoer gelegd door de procureur des Konings. Er wordt gehandeld overeenkomstig de artikelen 47ter tot 47novies. Alleen de onderzoeksrechter kan bovendien een observatie machtigen, zoals bedoeld in artikel 47sexies, met gebruik van technische hulpmiddelen om zicht te verwerven in een woning, of in de door deze woning omsloten eigen aanhorigheid in de zin van de artikelen 479, 480 en 481 van het Strafwetboek, of in een lokaal dat aangewend wordt voor beroepsdoeleinden of de woonplaats van een advocaat of een arts zoals bedoeld in het derde lid, wanneer er ernstige aanwijzingen zijn dat de strafbare feiten een misdrijf uitmaken of zouden uitmaken zoals bedoeld in artikel 90ter, §§ 2 tot 4, of gepleegd worden of zouden worden in het	In afwijking van artikel 56, § 1, derde lid, worden de machtigingen van de onderzoeksrechter waarbij hij bijzondere opsporingsmethoden **of een maatregel zoals bedoeld in artikel 46sexies** beveelt ten uitvoer gelegd door de procureur des Konings. Er wordt gehandeld overeenkomstig de artikelen 47ter tot 47novies, **respectievelijk artikel 46sexies.** Alleen de onderzoeksrechter kan bovendien een observatie machtigen, zoals bedoeld in artikel 47sexies, met gebruik van technische hulpmiddelen om zicht te verwerven in een woning, of in de door deze woning omsloten eigen aanhorigheid in de zin van de artikelen 479, 480 en 481 van het Strafwetboek, of in een lokaal dat aangewend wordt voor beroepsdoeleinden of de woonplaats van een advocaat of een arts zoals bedoeld in het derde lid, wanneer er ernstige aanwijzingen zijn dat de strafbare feiten een misdrijf uitmaken of zouden uitmaken zoals bedoeld in artikel 90ter, §§ 2 tot 4, of gepleegd worden of zouden worden in het

kader van een criminele organisatie zoals bedoeld in artikel 324bis van het Strafwetboek.	kader van een criminele organisatie zoals bedoeld in artikel 324bis van het Strafwetboek.
Een observatie zoals bedoeld in het vorige lid, een infiltratie zoals bedoeld in artikel 47octies of een inkijkoperatie zoals bedoeld in artikel 89ter, die betrekking hebben op de lokalen aangewend voor beroepsdoeleinden of de woonplaats van een advocaat of een arts, kunnen slechts door de onderzoeksrechter gemachtigd worden wanneer de advocaat of de arts er zelf van verdacht wordt één van de strafbare feiten bedoeld in artikel 90ter, §§ 2 tot 4, of een strafbaar feit in het kader van een criminele organisatie zoals bedoeld in artikel 324bis van het Strafwetboek gepleegd te hebben, of indien precieze feiten doen vermoeden dat derden die ervan verdacht worden één van deze strafbare feiten te hebben gepleegd, gebruik maken van diens lokalen of woonplaats.	Een observatie zoals bedoeld in het vorige lid, een infiltratie zoals bedoeld in artikel 47octies of een inkijkoperatie zoals bedoeld in artikel 89ter, die betrekking hebben op de lokalen aangewend voor beroepsdoeleinden of de woonplaats van een advocaat of een arts, kunnen slechts door de onderzoeksrechter gemachtigd worden wanneer de advocaat of de arts er zelf van verdacht wordt één van de strafbare feiten bedoeld in artikel 90ter, §§ 2 tot 4, of een strafbaar feit in het kader van een criminele organisatie zoals bedoeld in artikel 324bis van het Strafwetboek gepleegd te hebben, of indien precieze feiten doen vermoeden dat derden die ervan verdacht worden één van deze strafbare feiten te hebben gepleegd, gebruik maken van diens lokalen of woonplaats.
Deze maatregelen kunnen niet ten uitvoer worden gelegd zonder dat de stafhouder of de vertegenwoordiger van de provinciale orde van geneesheren ervan op de hoogte is.	Deze maatregelen kunnen niet ten uitvoer worden gelegd zonder dat de stafhouder of de vertegenwoordiger van de provinciale orde van geneesheren ervan op de hoogte is. **Deze personen zijn tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.**
De onderzoeksrechter heeft in zijn onderzoek steeds het recht het vertrouwelijk dossier aangaande de uitvoering van de bijzondere opsporingsmethodes in te zien, zonder dat hij van de inhoud ervan in het kader van zijn gerechtelijk onderzoek gewag kan maken. Hij kan steeds op gemotiveerde wijze de machtiging wijzigen, aanvullen of verlengen. Hij kan te allen tijde de machtiging intrekken. Hij gaat bij elke wijziging, aanvulling of verlenging van de machtiging na of de voorwaarden voor de bijzondere opsporingsmethode vervuld zijn.	De onderzoeksrechter heeft in zijn onderzoek steeds het recht het vertrouwelijk dossier aangaande de uitvoering van de bijzondere opsporingsmethodes in te zien, zonder dat hij van de inhoud ervan in het kader van zijn gerechtelijk onderzoek gewag kan maken. Hij kan steeds op gemotiveerde wijze de machtiging wijzigen, aanvullen of verlengen. Hij kan te allen tijde de machtiging intrekken. Hij gaat bij elke wijziging, aanvulling of verlenging van de machtiging na of de voorwaarden voor de bijzondere opsporingsmethode vervuld zijn.
De onderzoeksrechter bevestigt bij schriftelijk bevel het bestaan van de door hem verleende machtiging tot het uitvoeren van de bijzondere opsporingsmethode.	De onderzoeksrechter bevestigt bij schriftelijk bevel het bestaan van de door hem verleende machtiging tot het uitvoeren van de bijzondere opsporingsmethode.
De opgestelde processen-verbaal en het in het vorige lid bedoelde bevel worden uiterlijk na het beëindigen van de bijzondere	De opgestelde processen-verbaal en het in het vorige lid bedoelde bevel worden uiterlijk na het beëindigen van de bijzondere

opsporingsmethode bij het strafdossier gevoegd.	opsporingsmethode bij het strafdossier gevoegd.
Artikel 88bis	**Artikel 88bis**
§ 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 rechtstreeks of via een door de Koning aangewezen politiedienst de medewerking vorderen van de operator van een elektronisch communicatienetwerk of van de verstrekker van een elektronische communicatiedienst, om over te gaan of te doen overgaan tot:	§ 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:
1° de oproepgegevens doen opsporen van telecommunicatiemiddelen van waaruit of waarnaar oproepen worden of werden gedaan;	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 telecommunicatie laten lokaliseren.	2° de oorsprong of de bestemming van elektronische communicatie laten lokaliseren. **Hiertoe kan hij zo nodig, rechtstreeks of via de door de Koning aangewezen politiedienst, de medewerking vorderen van:** **- de operator van een elektronisch communicatienetwerk; en** **- iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.**
In de gevallen bepaald in het eerste lid wordt	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.	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 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.	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.
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.	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**, 434** 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.	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.	Indien het echter het in artikel 347bis**, 434** 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.	In spoedeisende gevallen kan de maatregel mondeling worden bevolen. Het bevel moet zo spoedig mogelijk worden bevestigd in de vorm bepaald in het vierde **en vijfde** 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 12 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 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.	§ 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 90ter, §§ 2 tot 4, of die gepleegd zijn in het kader van een criminele organisatie zoals bedoeld in artikel 324bis van het Strafwetboek, of die een gevangenisstraf van 5 jaar of een zwaardere straf tot gevolg kunnen hebben, kan de onderzoeksrechter in zijn bevelschrift de gegevens 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.
§ 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	§ 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.	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. **Deze personen zijn tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.**
§ 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.	§ 4. **De actoren bedoeld in § 1, tweede lid, delen** de gegevens waarom verzocht werd mee **in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, volgens de modaliteiten vastgesteld** 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 aan de vorderingen bedoeld in dit artikel weigert **of niet verleent in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering**, 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.
Artikel 88ter	**Artikel 88ter**
§ 1. Wanneer de onderzoeksrechter een zoeking beveelt in een informaticasysteem of een deel daarvan, kan deze zoeking worden uitgebreid naar een informaticasysteem of	Geschrapt

een deel daarvan dat zich op een andere plaats bevindt dan daar waar de zoeking plaatsvindt : - indien deze uitbreiding noodzakelijk is om de waarheid aan het licht te brengen ten aanzien van het misdrijf dat het voorwerp uitmaakt van de zoeking; en - indien andere maatregelen disproportioneel zouden zijn, of indien er een risico bestaat dat zonder deze uitbreiding bewijselementen verloren gaan. § 2. De uitbreiding van de zoeking in een informaticasysteem mag zich niet verder uitstrekken dan tot de informaticasystemen of de delen daarvan waartoe de personen die gerechtigd zijn het onderzochte informaticasysteem te gebruiken, in het bijzonder toegang hebben. § 3. Inzake de door uitbreiding van de zoeking in een informaticasysteem aangetroffen gegevens, die nuttig zijn voor dezelfde doeleinden als de inbeslagneming, wordt gehandeld zoals bepaald in artikel 39bis. De onderzoeksrechter brengt de verantwoordelijke van dit informaticasysteem op de hoogte, tenzij diens identiteit of woonplaats redelijkerwijze niet achterhaald kan worden. Wanneer blijkt dat deze gegevens zich niet op het grondgebied van het Rijk bevinden, worden ze enkel gekopieerd. In dat geval deelt de onderzoeksrechter dit, via het openbaar ministerie, onverwijld mee aan het ministerie van Justitie, dat de bevoegde overheid van de betrokken Staat hiervan op de hoogte brengt, indien deze redelijkerwijze kan worden bepaald. § 4. Artikel 89bis is van toepassing op de uitbreiding van de zoeking in een informaticasysteem.	
Artikel 88quater	**Artikel 88quater**
§ 1. De onderzoeksrechter, of in zijn opdracht een officier van gerechtelijke politie, hulpofficier van de procureur des Konings en van de arbeidsauditeur, kan personen van wie hij vermoedt dat ze een bijzondere kennis hebben van het informaticasysteem dat het voorwerp uitmaakt van de zoeking of	§ 1. De onderzoeksrechter, of in zijn opdracht een officier van gerechtelijke politie, hulpofficier van de procureur des Konings en van de arbeidsauditeur, kan **aan eenieder** van wie hij vermoedt dat ze een bijzondere kennis hebben van het informaticasysteem dat het voorwerp uitmaakt van de zoeking **of**

van diensten om gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem, te beveiligen of te versleutelen, bevelen inlichtingen te verstrekken over de werking ervan en over de wijze om er toegang toe te verkrijgen, of in een verstaanbare vorm toegang te verkrijgen tot de gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen. De onderzoeksrechter vermeldt de omstandigheden eigen aan de zaak die de maatregel wettigen in een met redenen omkleed bevelschrift dat hij meedeelt aan de procureur des Konings of aan de arbeidsauditeur.	**de uitbreiding ervan zoals bedoeld in artikel 39bis** of van diensten om gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem, te beveiligen of te versleutelen, bevelen inlichtingen te verstrekken over de werking ervan en over de wijze om er toegang toe te verkrijgen, of in een verstaanbare vorm toegang te verkrijgen tot de gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen. De onderzoeksrechter vermeldt de omstandigheden eigen aan de zaak die de maatregel wettigen in een met redenen omkleed bevelschrift dat hij meedeelt aan de procureur des Konings of aan de arbeidsauditeur.
§ 2. De onderzoeksrechter, of een door hem afgevaardigd officier van gerechtelijke politie, hulpofficier van de procureur des Konings en van de arbeidsauditeur,][1] kan iedere geschikte persoon bevelen om zelf het informaticasysteem te bedienen of de ter zake dienende gegevens, die door middel daarvan worden opgeslagen, verwerkt of overgedragen, naargelang het geval, te zoeken, toegankelijk te maken, te kopiëren, ontoegankelijk te maken of te verwijderen, in de door hem gevorderde vorm. Deze personen zijn verplicht hieraan gevolg te geven, voorzover dit in hun mogelijkheden ligt. Het bevel bedoeld in het eerste lid kan niet worden gegeven aan de verdachte en aan de personen bedoeld in artikel 156.	§ 2. De onderzoeksrechter, of een door hem afgevaardigd officier van gerechtelijke politie, hulpofficier van de procureur des Konings en van de arbeidsauditeur, kan iedere geschikte persoon bevelen om zelf het informaticasysteem te bedienen of de ter zake dienende gegevens, die door middel daarvan worden opgeslagen, verwerkt of overgedragen, naargelang het geval, te zoeken, toegankelijk te maken, te kopiëren, ontoegankelijk te maken of te verwijderen, in de door hem gevorderde vorm. Deze personen zijn verplicht hieraan gevolg te geven, voorzover dit in hun mogelijkheden ligt. Dit bevel kan niet worden gegeven aan de verdachte en aan de personen bedoeld in artikel 156.
§ 3. Hij die weigert de in §§1 en 2 gevorderde medewerking te verlenen of de zoeking in het informaticasysteem hindert, wordt gestraft met gevangenisstraf van zes maanden tot één jaar en met geldboete van zesentwintig frank tot twintigduizend frank of met een van die straffen alleen.	§3. Hij die de in §§ 1 en 2 gevorderde medewerking niet verleent of de zoeking in het informaticasysteem **of de uitbreiding ervan** hindert, wordt gestraft met gevangenisstraf van zes maanden tot **drie jaar** en met geldboete van zesentwintig frank tot twintigduizend frank of met een van die straffen alleen. **Wanneer de medewerking bedoeld in het eerste lid de uitvoering van een misdaad of een wanbedrijf kan verhinderen, of de gevolgen ervan kan beperken, en deze medewerking niet verleend wordt, zijn de straffen een gevangenisstraf van één tot vijf jaar en een geldboete van vijfhonderd**

	tot vijftigduizend frank.
§ 4. Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.	§ 4. Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.
§ 5. De Staat is burgerrechtelijk aansprakelijk voor de schade die onopzettelijk door de gevorderde personen aan een informaticasysteem of de gegevens. die door middel daarvan worden opgeslagen, verwerkt of overgedragen, wordt veroorzaakt.	§ 5. De Staat is burgerrechtelijk aansprakelijk voor de schade die onopzettelijk door de gevorderde personen aan een informaticasysteem of de gegevens. die door middel daarvan worden opgeslagen, verwerkt of overgedragen, wordt veroorzaakt.
Artikel 89ter	**Artikel 89ter**
In het kader van de uitvoering van de in artikel 46quinquies bepaalde maatregel, en onder de voorwaarden daar vermeld, kan alleen de onderzoeksrechter de politiediensten machtigen om buiten medeweten van de eigenaar of van zijn rechthebbende, of van de bewoner, of zonder hun toestemming, te allen tijde een andere private plaats dan die welke bedoeld is artikel 46quinquies, § 1, te betreden.	In het kader van de uitvoering van de in artikel 46quinquies bepaalde maatregel, en onder de voorwaarden **en met het oog op de doeleinden** daar vermeld, kan alleen de onderzoeksrechter de politiedienst **aangewezen door de Koning** machtigen om: - buiten medeweten van de eigenaar of van zijn rechthebbende, of van de bewoner, of zonder hun toestemming, te allen tijde een andere private plaats dan die welke bedoeld is artikel 46quinquies, § 1, te betreden, **met inbegrip van het openen van gesloten voorwerpen die zich op deze plaats bevinden;** - **buiten medeweten van de eigenaar, de bezitter of de gebruiker of zonder hun toestemming, zich toegang te verschaffen tot een informaticasysteem en het te doorzoeken, onverminderd de mogelijkheid voor de procureur des Konings om het binnendringen in een informaticasysteem te machtigen binnen de grenzen bepaald in artikel 46quinquies, § 6.**
Ingeval de in het eerste lid bedoelde machtiging wordt verleend in het kader van de toepassing van bijzondere opsporingsmethoden overeenkomstig de artikelen 47ter tot 47decies of artikel 56bis,	Ingeval de in het eerste lid bedoelde machtiging wordt verleend in het kader van de toepassing van bijzondere opsporingsmethoden overeenkomstig de artikelen 47ter tot 47decies of artikel 56bis,

worden de machtiging en alle ermee verband houdende processen-verbaal uiterlijk na het beëindigen van de bijzondere opsporingsmethode bij het strafdossier gevoegd. Hij deelt een kopie van dit bevel aan de procureur des Konings mee.	worden de machtiging en alle ermee verband houdende processen-verbaal uiterlijk na het beëindigen van de bijzondere opsporingsmethode bij het strafdossier gevoegd. Hij deelt een kopie van dit bevel aan de procureur des Konings mee.
§ 6. AFLUISTEREN, KENNISNEMEN OPNEMEN VAN PRIVECOMMUNICATIE TELECOMMUNICATIE	**§ 6. ONDERSCHEPPEN, KENNISNEMEN, DOORZOEKEN EN OPNEMEN VAN NIET VOOR PUBLIEK TOEGANKELIJKE COMMUNICATIE OF GEGEVENS VAN EEN INFORMATICASYSTEEM OF EEN DEEL ERVAN.**
Artikel 90ter	**Artikel 90ter**
§ 1. De onderzoeksrechter kan in uitzonderlijke gevallen, wanneer het onderzoek zulks vereist, privé-communicatie of -telecommunicatie, tijdens de overbrenging ervan, afluisteren, er kennis van nemen en opnemen, indien er ernstige aanwijzingen bestaan dat het feit waarvoor hij geadieerd is een strafbaar feit is, bedoeld in een van de bepalingen opgesomd in § 2, en indien de overige middelen van onderzoek niet volstaan om de waarheid aan de dag te brengen. Teneinde het mogelijk te maken om privé-communicatie of -telecommunicatie direct af te luisteren, er kennis van te nemen of op te nemen met technische hulpmiddelen, kan de onderzoeksrechter bevelen om, te allen tijde, ook buiten medeweten of zonder de toestemming van hetzij de bewoner, hetzij de eigenaar of zijn rechthebbende, in een woning of in een private plaats binnen te dringen.	§ 1. **De onderzoeksrechter kan, onverminderd de toepassing van artikelen 39bis, 87, 88, 89bis en 90, met een heimelijk oogmerk, niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem of een deel ervan met technische hulpmiddelen onderscheppen, er kennis van nemen, doorzoeken en opnemen of de zoeking in een informaticasysteem of een deel ervan uitbreiden.** **Deze maatregel kan enkel worden bevolen in uitzonderlijke gevallen, wanneer het onderzoek zulks vereist, indien er ernstige aanwijzingen bestaan dat het een strafbaar feit betreft bedoeld in een van de bepalingen opgesomd in § 2, en indien de overige middelen van onderzoek niet volstaan om de waarheid aan de dag te brengen.** Teneinde **deze maatregel** mogelijk te maken, kan de onderzoeksrechter bevelen om, te allen tijde, ook buiten medeweten of zonder de toestemming van hetzij de bewoner, hetzij de eigenaar of zijn rechthebbende**, hetzij de gebruiker:** **- in een woning, in een private plaats of in een informaticasysteem binnen te dringen;** **- elke beveiliging van de betrokken informaticasystemen tijdelijk op te heffen,**

	desgevallend met behulp van technische hulpmiddelen, valse signalen, valse sleutels of valse hoedanigheden; **- technische middelen in de betrokken informaticasystemen aan te brengen teneinde de door dat systeem opgeslagen, verwerkte of doorgestuurde gegevens te ontcijferen en te decoderen**
De bewakingsmaatregel kan alleen worden bevolen ten aanzien van personen die op grond van precieze aanwijzingen ervan verdacht worden het strafbare feit te hebben gepleegd, ten aanzien van de communicatie- of telecommunicatiemiddelen die geregeld worden gebruikt door een persoon op wie een verdenking rust, of ten aanzien van de plaatsen waar deze vermoed wordt te vertoeven. De maatregel kan eveneens worden bevolen ten aanzien van personen van wie op grond van precieze feiten vermoed wordt dat zij geregeld in verbinding staan met een persoon op wie een verdenking rust.	**De maatregel bedoeld in deze paragraaf kan alleen worden bevolen om de gegevens op te sporen die kunnen dienen om de waarheid aan de dag te brengen. Hij kan** alleen worden bevolen ten aanzien van personen die op grond van precieze aanwijzingen ervan verdacht worden het strafbare feit te hebben gepleegd, ten aanzien van de communicatiemiddelen of informaticasystemen die geregeld worden gebruikt door een persoon op wie een verdenking rust of ten aanzien van de plaatsen waar deze vermoed wordt te vertoeven. De maatregel kan eveneens worden bevolen ten aanzien van personen van wie op grond van precieze feiten vermoed wordt dat zij geregeld in verbinding staan met een persoon op wie een verdenking rust.
§ 2. De strafbare feiten die een bewakingsmaatregel kunnen wettigen, zijn die welke bedoeld zijn in:	§ 2. De strafbare feiten die **de maatregel bedoeld in §1** kunnen wettigen zijn degene die bedoeld worden in:
1° de artikelen 101 tot en met 110 van het Strafwetboek;	1° de artikelen 101 tot en met 110 van het Strafwetboek;
1°bis. De artikelen 136bis, 136ter, 136quater, 136sexies en 136septies van hetzelfde Wetboek en artikel 41 van de wet van 29 maart 2004 betreffende de samenwerking met het Internationaal Strafgerechtshof en de internationale straftribunalen;	**2°** De artikelen 136bis, 136ter, 136quater, 136sexies en 136septies van hetzelfde Wetboek en artikel 41 van de wet van 29 maart 2004 betreffende de samenwerking met het Internationaal Strafgerechtshof en de internationale straftribunalen;
1°ter boek II, titel Iter, van hetzelfde Wetboek;	**3°** Boek II, Titel Iter, van hetzelfde Wetboek; **4° artikel 147 van hetzelfde Wetboek**; **5° de artikelen 160, 161, 162, 163, 168, 171, 173 en 176 van hetzelfde Wetboek**; **6° de artikelen 180 en 186 van hetzelfde**

	Wetboek;
1°quater artikel 210bis van hetzelfde Wetboek;	**7°** artikel 210bis van hetzelfde Wetboek;
1°quinquies de artikelen 246, 247, 248, 249, 250 en 251 van hetzelfde Wetboek;	**8°** de artikelen 246, 247, 248, 249, en 250 van hetzelfde Wetboek;
1°sexies artikel 259bis van hetzelfde Wetboek;	**9°** artikel 259bis van hetzelfde Wetboek;
1°septies artikel 314bis van hetzelfde Wetboek;	**10°** artikel 314bis van hetzelfde Wetboek;
1°octies de artikelen 324bis en 324ter van hetzelfde Wetboek	**11°** de artikelen 324bis en 324ter van hetzelfde Wetboek;
2° de artikelen 327, 328, 329 of 330 van hetzelfde Wetboek, voor zover een klacht is ingediend;	**12°** de artikelen 327, 328, 329 of 330 van hetzelfde Wetboek, voor zover een klacht is ingediend;
3° artikel 331bis van hetzelfde Wetboek;	**13°** artikel 331bis van hetzelfde Wetboek;
4° artikel 347bis van hetzelfde Wetboek;	**14°** artikel 347bis van hetzelfde Wetboek;
4°bis	**15° de artikelen 372 tot 377bis van hetzelfde Wetboek**;
	16° artikel 377quater van hetzelfde Wetboek;
5° De artikelen 379 en 380 van hetzelfde Wetboek.	**17°** de artikelen 379, 380 **en 383bis, §1 en 3** van hetzelfde Wetboek;
6° artikel 393 van hetzelfde Wetboek;	**18°** artikel 393 van hetzelfde Wetboek;
7° de artikelen 394 of 397 van hetzelfde Wetboek;	**19°** de artikelen 394 of 397 van hetzelfde Wetboek;
7°bis. de artikelen 428 en 429 van hetzelfde Wetboek;	**20°** de artikelen 428 en 429 van hetzelfde Wetboek;
	21° artikel 433bis/1 van hetzelfde Wetboek;
7°ter. de artikelen 433sexies, 433septies en 433octies van hetzelfde Wetboek;	**22°** de artikelen **433quinquies tot** 433octies van hetzelfde Wetboek;
	23° artikel 434 van hetzelfde Wetboek;
8°de artikelen 468, 470, 471 of 472 van hetzelfde Wetboek;	**24°** de artikelen 468, 470, 471 of 472 van hetzelfde Wetboek;
9° artikel 475 van hetzelfde Wetboek;	**25°** artikel 475 van hetzelfde Wetboek;
10° de artikelen 477, 477bis, 477ter,	

477quater, 477quinquies, 477sexies of 488bis van hetzelfde Wetboek;	**26°** boek II, titel IX, hoofdstuk I, sectie 2bis, en hoofdstuk Ibis van hetzelfde Wetboek;
10°bis. De artikelen 504bis en 504ter van hetzelfde Wetboek;	**27°** de artikelen 504bis en 504ter van hetzelfde Wetboek;
10°ter. Artikel 504quater van hetzelfde Wetboek.	**28°** artikel 504quater van hetzelfde Wetboek;
11° artikel 505, eerste lid, 2°, 3° en 4° van hetzelfde Wetboek;	**29° artikel 505, eerste lid, 1° van hetzelfde Wetboek wanneer de betrokken zaken werden weggenomen, verduisterd of verkregen door een misdaad of wanbedrijf vermeld in dit artikel;**
	30° artikel 505, eerste lid, 2°, 3° en 4° van hetzelfde Wetboek;
12° de artikelen 510, 511, eerste lid of 516 van hetzelfde Wetboek;	**31°** de artikelen 510, 511, eerste lid of 516 van hetzelfde Wetboek;
13° artikel 520 van hetzelfde Wetboek, indien de omstandigheden bedoeld in de artikelen 510 of 511, eerste lid, van hetzelfde Wetboek verenigd zijn;	**32°** artikel 520 van hetzelfde Wetboek, indien de omstandigheden bedoeld in de artikelen 510 of 511, eerste lid, van hetzelfde Wetboek verenigd zijn;
13°bis Artikelen 550bis en 550ter van hetzelfde Wetboek.	**33°** artikelen 550bis en 550ter van hetzelfde Wetboek;
14° artikel 2bis, § 3, b, of § 4, b, van de wet van 24 februari 1921 betreffende het verhandelen van de giftstoffen, slaapmiddelen en verdovende middelen, ontsmettingsstoffen en antiseptica; 1	**34°** artikel 2bis van de wet van 24 februari 1921 betreffende het verhandelen van giftstoffen, slaapmiddelen en verdovende middelen, psychotrope stoffen, ontsmettingsstoffen en antiseptica **en van de stoffen die kunnen gebruikt worden voor de illegale vervaardiging van verdovende middelen en psychotrope stoffen**;
15° artikel 145, § 3 en § 3bis van de wet van 13 juni 2005 betreffende de elektronische communicatie;	**35°** artikel 145, § 3 en § 3bis van de wet van 13 juni 2005 betreffende de elektronische communicatie;
16° artikel 10 van de wet van 5 augustus 1991 betreffende de in-, uit- en doorvoer van wapens, munitie en speciaal voor militair gebruik dienstig materieel en daaraan verbonden technologie.	**36°** artikel 10 van de wet van 5 augustus 1991 betreffende de in-, uit- en doorvoer van wapens, munitie en speciaal voor militair gebruik dienstig materieel en daaraan verbonden technologie;
16bis° artikel 47 van het decreet van het Vlaams Parlement van 15 juni 2012 betreffende de in-, uit-, doorvoer en overbrenging van defensiegerelateerde producten, ander voor militair gebruik dienstig materiaal, ordehandhavingsmateriaal, civiele	**37°** artikel 47 van het decreet van het Vlaams Parlement van 15 juni 2012 betreffende de in-, uit-, doorvoer en overbrenging van defensiegerelateerde producten, ander voor militair gebruik dienstig materiaal,

vuurwapens, onderdelen en munitie;	ordehandhavingsmateriaal, civiele vuurwapens, onderdelen en munitie;
16ter° artikel 20 van het decreet van het Waals Gewest van 21 juni 2012 betreffende de invoer, uitvoer, doorvoer en overdracht van civiele wapens en van defensiegerelateerde producten;	**38°** artikel 20 van het decreet van het Waals Gewest van 21 juni 2012 betreffende de invoer, uitvoer, doorvoer en overdracht van civiele wapens en van defensiegerelateerde producten;
16quater° artikel 42 van de ordonnantie van het Brussels Hoofdstedelijk gewest van 20 juni 2013 betreffende de in-, uit-, doorvoer en overbrenging van defensiegerelateerde producten, ander voor militair gebruik dienstig materiaal, ordehandhavingsmateriaal, civiele vuurwapens, onderdelen, toebehoren en munitie ervan;	**39°** artikel 42 van de ordonnantie van het Brussels Hoofdstedelijk gewest van 20 juni 2013 betreffende de in-, uit-, doorvoer en overbrenging van defensiegerelateerde producten, ander voor militair gebruik dienstig materiaal, ordehandhavingsmateriaal, civiele vuurwapens, onderdelen, toebehoren en munitie ervan;
16quinquies° artikelen 8 tot 11, 14, 16, 19, 1°, 2°, 3°, 5° en 6°, 20, 22, 27 en 33 van de wet van 8 juni 2006 houdende regeling van economische en individuele activiteiten met wapens, ook « wapenwet » genoemd;	**40°** artikelen 8 tot 11, 14, 16, 19, 1°, 2°, 3°, 5° en 6°, 20, 22, 27 en 33 van de wet van 8 juni 2006 houdende regeling van economische en individuele activiteiten met wapens, ook « wapenwet » genoemd;
16sexies° de wet van 28 mei 1956 betreffende ontplofbare en voor de deflagratie vatbare stoffen en mengsels en de daarmede geladen tuigen;	**41°** de wet van 28 mei 1956 betreffende ontplofbare en voor de deflagratie vatbare stoffen en mengsels en de daarmede geladen tuigen;
16septies° artikelen 21 tot 26 van het Samenwerkingsakkoord tussen de federale Staat, het Vlaams Gewest, het Waals Gewest en het Brussels Hoofdstedelijk Gewest betreffende de uitvoering van de overeenkomst tot verbod van de ontwikkeling, de productie, de aanleg van voorraden en het gebruik van chemische wapens en inzake de vernietiging van deze wapens, gedaan te Parijs op 13 januari 1993;	**42°** artikelen 21 tot 26 van het Samenwerkingsakkoord tussen de federale Staat, het Vlaams Gewest, het Waals Gewest en het Brussels Hoofdstedelijk Gewest betreffende de uitvoering van de overeenkomst tot verbod van de ontwikkeling, de productie, de aanleg van voorraden en het gebruik van chemische wapens en inzake de vernietiging van deze wapens, gedaan te Parijs op 13 januari 1993;
17° de artikelen 77ter, 77quater en 77quinquies van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen;	**43**° de artikelen **77bis tot** 77quinquies van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen;
18° artikel 10, § 1, 2°, van de wet van 15 juli 1985 betreffende het gebruik bij dieren van stoffen met hormonale, anti-hormonale, beta-adrenergische of productie-stimulerende werking;	**44**° artikel 10, § 1, 2°, van de wet van 15 juli 1985 betreffende het gebruik bij dieren van stoffen met hormonale, anti-hormonale, beta-adrenergische of productie-stimulerende werking;
19° artikel 1 van het koninklijk besluit van 12 april 1974 betreffende sommige	**45**° artikel 1 van het koninklijk besluit van 12

verrichtingen in verband met stoffen met hormonale, anti-hormonale, anabole, anti-infectieuze, anti-parasitaire, en anti-inflammatoire werking, welk artikel betrekking heeft op strafbare feiten waarop overeenkomstig de wet van 24 februari 1921 betreffende het verhandelen van de gifstoffen, slaapmiddelen en verdovende middelen, ontsmettingsstoffen en antiseptica straffen worden gesteld;	april 1974 betreffende sommige verrichtingen in verband met stoffen met hormonale, anti-hormonale, anabole, anti-infectieuze, anti-parasitaire, en anti-inflammatoire werking, welk artikel betrekking heeft op strafbare feiten waarop overeenkomstig de wet van 24 februari 1921 betreffende het verhandelen van de gifstoffen, slaapmiddelen en verdovende middelen, ontsmettingsstoffen en antiseptica straffen worden gesteld;
§ 3. Poging tot het plegen van een misdaad bedoeld in de voorgaande paragraaf kan eveneens een bewakingsmaatregel wettigen.	§ 3. Poging tot het plegen van een misdaad bedoeld in de voorgaande paragraaf kan eveneens een maatregel wettigen.
§ 4. Een strafbaar feit, bedoeld in de artikelen 322 of 323 van het Strafwetboek, kan eveneens een bewakingsmaatregel wettigen, voor zover de vereniging gevormd is met het doel een aanslag te plegen tegen de personen of eigendommen bedoeld in § 2 of om het in artikel 467, eerste lid, van het Strafwetboek bedoelde strafbare feit te begaan.	§ 4. Een strafbaar feit, bedoeld in de artikelen 322 of 323 van het Strafwetboek, kan eveneens een maatregel wettigen, voor zover de vereniging gevormd is met het doel een aanslag te plegen tegen de personen of eigendommen bedoeld in § 2 of om het in artikel 467, eerste lid, van het Strafwetboek bedoelde strafbare feit te begaan.
§ 5. In geval van ontdekking op heterdaad en zolang de heterdaadsituatie duurt, kan de procureur des Konings de in § 1 bedoelde maatregel bevelen voor de in artikel 347bis of 470 van het Strafwetboek bedoelde strafbare feiten.	§ 5. Ingeval van ontdekking op heterdaad en zolang de heterdaadsituatie duurt, kan de procureur des Konings de maatregel bedoeld in § 1, eerste lid, bevelen voor de strafbare feiten bedoeld in de **artikelen 347bis, 434, of 470 van het Strafwetboek**.
§ 6. Een bevoegde buitenlandse overheid mag, in het raam van een strafrechtelijk onderzoek, tijdelijk privé-telecommunicatie afluisteren, er kennis van nemen en opnemen tijdens de overbrenging ervan, ingeval de persoon op wie deze maatregel betrekking heeft, zich op het Belgische grondgebied bevindt en indien voldaan is aan de volgende voorwaarden :	§ 6. Een bevoegde buitenlandse overheid mag, in het raam van een strafrechtelijk onderzoek, **tijdelijk niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem onderscheppen**, er kennis van nemen en opnemen, ingeval de persoon op wie deze maatregel betrekking heeft, zich op het Belgische grondgebied bevindt en indien voldaan is aan de volgende voorwaarden:
1° deze maatregel vereist geen technische tussenkomst van een instantie die in België is gevestigd; 2° de betrokken buitenlandse overheid heeft kennis gegeven van deze maatregel aan een Belgische rechterlijke overheid; 3° in deze mogelijkheid is voorzien in een internationaal rechtsinstrument tussen België en de verzoekende Staat; 4° de in § 7 bedoelde beslissing van de onderzoeksrechter is nog niet meegedeeld aan de betrokken buitenlandse overheid.	1° deze maatregel vereist geen technische tussenkomst van een instantie die in België is gevestigd 2° de betrokken buitenlandse overheid heeft kennis gegeven van deze maatregel aan een Belgische rechterlijke overheid; 3° in deze mogelijkheid is voorzien in een internationaal rechtsinstrument tussen België en de verzoekende Staat; 4° de in § 7 bedoelde beslissing van de onderzoeksrechter is nog niet meegedeeld

	aan de betrokken buitenlandse overheid.
De gegevens die op grond van deze paragraaf zijn verzameld, kunnen alleen worden gebruikt op voorwaarde dat de bevoegde Belgische rechterlijke overheid instemt met de maatregel.	De gegevens die op grond van deze paragraaf zijn verzameld, kunnen alleen worden gebruikt op voorwaarde dat de bevoegde Belgische rechterlijke overheid instemt met de maatregel.
§ 7. Zodra de procureur des Konings de in paragraaf 6, eerste lid, 2°, bedoelde kennisgeving ontvangt, maakt hij ze onverwijld aanhangig bij de onderzoeksrechter.	§ 7. Zodra de procureur des Konings de in paragraaf 6, eerste lid, 2°, bedoelde kennisgeving ontvangt, maakt hij ze onverwijld aanhangig bij de onderzoeksrechter.
De onderzoeksrechter bij wie een kennisgeving als bedoeld in § 6, eerste lid, 2°, aanhangig is gemaakt, stemt in met de betrokken maatregel indien deze toelaatbaar is overeenkomstig het bepaalde in dit artikel.	De onderzoeksrechter bij wie een kennisgeving als bedoeld in § 6, eerste lid, 2°, aanhangig is gemaakt, stemt in met de betrokken maatregel indien deze toelaatbaar is overeenkomstig het bepaalde in dit artikel.
Hij stelt de betrokken buitenlandse overheid in kennis van zijn beslissing binnen zesennegentig uur vanaf de ontvangst ervan door de Belgische gerechtelijke overheid.	Hij stelt de betrokken buitenlandse overheid in kennis van zijn beslissing binnen zesennegentig uur vanaf de ontvangst ervan door de Belgische gerechtelijke overheid.
Ingeval een bijkomende termijn noodzakelijk is, kan de onderzoeksrechter zijn beslissing en de kennisgeving ervan aan de bevoegde buitenlandse overheid maximum acht dagen uitstellen. Hij verwittigt hiervan onverwijld de bevoegde buitenlandse overheid met opgave van de redenen.	Ingeval een bijkomende termijn noodzakelijk is, kan de onderzoeksrechter zijn beslissing en de kennisgeving ervan aan de bevoegde buitenlandse overheid maximum acht dagen uitstellen. Hij verwittigt hiervan onverwijld de bevoegde buitenlandse overheid met opgave van de redenen.
Ingeval de onderzoeksrechter de in § 6 bedoelde maatregel niet toestaat, deelt hij de buitenlandse overheid eveneens mee dat de verkregen gegevens moeten worden vernietigd zonder te kunnen worden gebruikt.	Ingeval de onderzoeksrechter de in § 6 bedoelde maatregel niet toestaat, deelt hij de buitenlandse overheid eveneens mee dat de verkregen gegevens moeten worden vernietigd zonder te kunnen worden gebruikt.
Artikel 90quater	**Artikel 90quater**
§ 1. Tot iedere bewakingsmaatregel op grond van artikel 90ter wordt vooraf machtiging verleend bij een met redenen omklede beschikking van de onderzoeksrechter die de beschikking aan de procureur des Konings meedeelt.	§ 1. Tot iedere **maatregel** op grond van artikel 90ter **verleent de onderzoeksrechter een schriftelijke voorafgaande met redenen omklede machtiging die hij meedeelt aan de procureur des Konings**.
De beschikking wordt gedagtekend en vermeldt:	De **machtiging** wordt gedagtekend en vermeldt:
1° de aanwijzigingen en de concrete feiten, eigen aan de zaak, die de maatregel	1° de aanwijzingen en de concrete feiten, eigen aan de zaak, die de maatregel

wettigen overeenkomstig artikel 90ter;	wettigen overeenkomstig artikel 90ter;
2° de redenen waarom de maatregel onontbeerlijk is om de waarheid aan de dag te brengen;	2° de redenen waarom de maatregel onontbeerlijk is om de waarheid aan de dag te brengen;
3° de persoon, het communicatie- of telecommunicatiemiddel of de plaats die het voorwerp is van de bewaking;	3° de persoon, het communicatiemiddel, het informaticasysteem of de plaats die het voorwerp is van de bewaking;
4° de periode tijdens welke de bewaking kan worden uitgeoefend, welke niet langer mag zijn dan één maand te rekenen van de beslissing waarbij de maatregel wordt bevolen;	4° **de periode tijdens dewelke de maatregel kan worden uitgeoefend, die niet langer mag zijn dan één maand. Deze termijn vangt aan de dag van de machtiging waarbij de maatregel wordt bevolen, of, ingeval van artikel 90quinquies, eerste lid, verlengd, en loopt tot en met de dag voor de zoveelste van de daarop volgende maand;**
5° de naam en de hoedanigheid van de officier van gerechtelijke politie aangewezen voor de uitvoering van de maatregel.	5° de naam en de hoedanigheid van de officier of officieren van gerechtelijke politie aangewezen voor de uitvoering van de maatregel. **In spoedeisende gevallen kan de machtiging mondeling worden verleend. Deze machtiging moet uiterlijk binnen vierentwintig uren worden bevestigd in de vorm bepaald in het tweede lid.**
§ 2. Indien de maatregel een bewerking op een communicatienetwerk inhoudt, is de operator van dit netwerk of de verstrekker van de telecommunicatiedienst ertoe gehouden zijn technische medewerking te verlenen, wanneer de onderzoeksrechter hierom rechtstreeks of via de tussenkomst van een politiedienst aangewezen door de Koning verzoekt.	§ 2. **De onderzoeksrechter kan, om de maatregel bedoeld in artikel 90ter, § 1, mogelijk te maken, rechtstreeks of via de tussenkomst van een politiedienst aangewezen door de Koning, de medewerking vorderen van:** - de operator van een elektronisch communicatienetwerk, en - **iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.**

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.
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.	Iedere persoon die zijn technische medewerking aan de vorderingen bedoeld in de vorige leden weigert **of niet verleent in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering**, 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 **twintigduizend** frank.
§ 3. De onderzoeksrechter mag voor de tenuitvoerlegging van zijn beschikking alleen officieren van gerechtelijke politie aanwijzen, die zich echter kunnen laten bijstaan door agenten van gerechtelijke politie wier namen vooraf aan de onderzoeksrechter worden meegedeeld. De namen van de agenten van gerechtelijke politie belast met de uitvoering van het bevel bedoeld in artikel 90ter, § 1, tweede lid, worden niet vermeld in het gerechtelijk dossier.	§ 3. De onderzoeksrechter mag voor de tenuitvoerlegging **van de maatregel bedoeld in artikel 90ter, § 1** alleen officieren van gerechtelijke politie aanwijzen. **Deze kunnen** zich echter laten bijstaan door agenten van gerechtelijke politie **en, onder de voorwaarden door de Koning bepaald, door personeelsleden van het administratief en logistiek kader van de geïntegreerde politie. De laatstgenoemde personen mogen niet belast worden met de analyse van de inhoud van de opgenomen communicatie of gegevens, tenzij het een specifieke expertise betreft, of met de selectie van voor het onderzoek relevant geachte delen, zoals bedoeld in artikel 90sexies, §1, 2°.** **De officieren van gerechtelijke politie houden de namen bij van de personen door wie zij zich laten bijstaan, in een lijst die voor elk dossier afzonderlijk wordt opgesteld volgens de modaliteiten door de Koning bepaald, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer. Indien deze personen belast zijn met de uitvoering van het bevel bedoeld in artikel 90ter, § 1, derde lid, worden hun namen niet vermeld in het gerechtelijk dossier.**
De aangewezen officieren van gerechtelijke politie brengen ten minste om de vijf dagen schriftelijk verslag uit aan de onderzoeksrechter over de tenuitvoerlegging	De aangewezen officieren van gerechtelijke politie brengen ten minste om de vijf dagen schriftelijk verslag uit aan de

van de beschikking.	onderzoeksrechter over de tenuitvoerlegging van de beschikking.
§ 4. De onderzoeksrechter kan personen waarvan hij vermoedt dat ze een bijzondere kennis hebben van de telecommunicatiedienst waarop de bewakingsmaatregel betrekking heeft of van diensten om gegevens, die worden opgeslagen, verwerkt of overgedragen via een informaticasysteem, te beveiligen of te versleutelen, rechtstreeks of via de tussenkomst van een politiedienst aangewezen door de Koning, bevelen inlichtingen te verlenen over de werking ervan en over de wijze om in een verstaanbare vorm toegang te verkrijgen tot de inhoud van telecommunicatie die wordt of is overgebracht.	§ 4. De onderzoeksrechter kan personen waarvan hij vermoedt dat ze een bijzondere kennis hebben van het communicatiemiddel of het informaticasysteem waarop de maatregel betrekking heeft of van diensten of toepassingen om gegevens, die worden opgeslagen, verwerkt of overgedragen via **een communicatiemiddel of** een informaticasysteem, te beveiligen**, te coderen** of te versleutelen, **rechtstreeks of via de tussenkomst van een politiedienst aangewezen door de Koning, vorderen** inlichtingen te verlenen over de werking ervan en over de wijze om in een verstaanbare vorm toegang te verkrijgen tot de inhoud ervan die wordt of is overgebracht.
Hij kan personen bevelen om de inhoud van de telecommunicatie toegankelijk te maken in de door hem gevorderde vorm. Deze personen zijn verplicht hieraan gevolg te geven, voorzover dit in hun mogelijkheden ligt.	Hij kan personen **vorderen** om **deze** inhoud toegankelijk te maken in de door hem **gewenste** vorm.
Hij die weigert de overeenkomstig de vorige leden bevolen medewerking te verlenen, wordt gestraft met gevangenisstraf van zes maanden tot een jaar en met geldboete van zesentwintig frank tot twintigduizend frank of met een van die straffen alleen.	**Iedere persoon die zijn technische medewerking weigert aan de vorderingen bedoeld in de vorige leden**, wordt gestraft met gevangenisstraf van zes maanden tot een jaar en met geldboete van zesentwintig frank tot twintigduizend frank of met een van die straffen alleen.
Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of die ertoe wordt geroepen zijn technische medewerking te verlenen, is gebonden door het geheim van het gerechtelijk onderzoek. 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 **gevorderd wordt** zijn technische medewerking te verlenen, is **tot geheimhouding verplicht**. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek. **§ 5. In voorkomend geval is artikel 39bis, § 3, vierde lid toepasbaar op de gegevens, aangetroffen door een zoeking in een informaticasysteem met toepassing van artikel 90ter, § 1.**
Artikel 90quinquies	**Artikel 90quinquies**
De onderzoeksrechter kan de uitwerking van	De onderzoeksrechter kan de uitwerking van

zijn beschikking één of meer malen verlengen met een termijn die niet langer mag zijn dan één maand, met een maximum van zes maanden, onverminderd zijn beslissing om aan de maatregel een einde te maken zodra de omstandigheden die deze gewettigd hebben, verdwenen zijn.	de **machtiging bedoeld in artikel 90quater, § 1**, één of meer malen verlengen met een termijn die niet langer mag zijn dan één maand, met een maximum van zes maanden, onverminderd zijn beslissing om aan de maatregel een einde te maken zodra de omstandigheden die deze gewettigd hebben, verdwenen zijn. **Deze termijn van zes maanden vangt aan de dag van de eerste machtiging waarbij de maatregel wordt bevolen, en loopt tot en met de dag voor de zoveelste van de zesde daarop volgende maand. Indien de maatregel, wegens de technische voorbereiding ervan, daadwerkelijk werd aangevat op een latere dag dan deze van de eerste machtiging, vangt de termijn van zes maanden aan de dag van deze daadwerkelijke aanvatting en ten laatste twee maanden na de dag van de eerste machtiging.**
De bepalingen vervat in artikel 90quater, § 1, zijn toepasselijk op de verlenging bedoeld in het voorgaande lid. De beschikking vermeldt bovendien de precieze omstandigheden die de verlenging van de maatregel wettigen.	De bepalingen vervat in artikel 90quater, § 1, zijn toepasselijk op de verlenging bedoeld in het voorgaande lid. De **machtiging** vermeldt bovendien de precieze omstandigheden die de verlenging van de maatregel wettigen.
Indien nieuwe en ernstige omstandigheden de maatregelen bedoeld in artikel 90ter noodzakelijk maken, kan de onderzoeksrechter een nieuwe maatregel bevelen, met inachtneming van de formaliteiten omschreven in de artikelen 90ter en 90quater, in dat geval moet de beschikking de precieze nieuwe en ernstige omstandigheden vermelden die een nieuwe maatregel noodzakelijk maken en wettigen.	Indien nieuwe en ernstige omstandigheden de maatregelen bedoeld in artikel 90ter noodzakelijk maken, kan de onderzoeksrechter een nieuwe maatregel bevelen, met inachtneming van de formaliteiten omschreven in de artikelen 90ter en 90quater. In dat geval moet de **machtiging** de precieze nieuwe en ernstige omstandigheden vermelden die een nieuwe maatregel noodzakelijk maken en wettigen.
Artikel 90sexies	**Artikel 90sexies**
§ 1. De aangewezen officieren van gerechtelijke politie stellen aan de onderzoeksrechter ter beschikking :	§ 1. De aangewezen officieren van gerechtelijke politie stellen aan de onderzoeksrechter ter beschikking:
1° het bestand bevattende de opnames verricht als gevolg van de maatregelen genomen met toepassing van de artikelen 90ter, 90quater en 90quinquies;	1° Het bestand bevattende de **opgenomen niet voor publiek toegankelijke communicaties of gegevens van een informaticasysteem bekomen** als gevolg van de maatregelen genomen met toepassing van de artikelen 90ter, 90quater en 90quinquies;

2° de overschrijving van de door de aangewezen officieren van gerechtelijke politie voor het onderzoek van belang geachte gedeelten van de opgenomen communicaties of telecommunicaties, en de eventuele vertaling ervan;	2° De overschrijving **of weergave** van de door de aangewezen officieren van gerechtelijke politie voor het onderzoek van belang geachte gedeelten van de opgenomen communicaties of **gegevens**, en de eventuele vertaling ervan;
	3° **In voorkomend geval, de plaats van de gegevens, bedoeld in 2°, in het informaticasysteem;**
3° de loutere vermelding van de aangehaalde onderwerpen en van de identificatiegegevens van de gebruikte communicatiemiddelen wat betreft de niet van belang geachte communicaties of telecommunicaties.	**4° Een algemene beschrijving** van de **inhoud** en van de identificatiegegevens van de gebruikte communicatiemiddelen **of informaticasystemen** wat betreft de niet van belang geachte communicaties of **gegevens.**
§ 2. Onverminderd de selectie door de officieren van gerechtelijke politie bedoeld in paragraaf 1, beoordeelt de onderzoeksrechter welke gedeelten van alle opgenomen communicaties en telecommunicaties van belang zijn voor het onderzoek. In zoverre deze gedeelten van communicaties of telecommunicaties niet overgeschreven of vertaald zijn overeenkomstig paragraaf 1, worden zij bijkomend overgeschreven en vertaald. De onderzoeksrechter laat daarvan proces-verbaal opmaken.	§ 2. Onverminderd de selectie door de officieren van gerechtelijke politie bedoeld in § 1, beoordeelt de onderzoeksrechter welke gedeelten van alle opgenomen **niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem** van belang zijn voor het onderzoek. In zoverre deze gedeelten van **de communicatie of gegevens** niet overgeschreven**, weergegeven** of vertaald zijn overeenkomstig **§ 1**, moeten zij bijkomend overgeschreven, **weergegeven en eventueel** vertaald worden. De onderzoeksrechter laat daarvan proces-verbaal opmaken.
§ 3. De communicatie of telecommunicatie die onder het beroepsgeheim valt, wordt niet opgetekend in het proces-verbaal. Deze communicatie of telecommunicatie wordt in een bestand onder verzegelde omslag neergelegd ter griffie. Gaat het om personen bedoeld in artikel 90octies, eerste lid, dan wordt ter zake gehandeld overeenkomstig artikel 90octies, tweede lid.	§ 3. De **niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem** die onder het beroepsgeheim vallen, worden niet opgetekend in het proces-verbaal. **Deze communicatie of gegevens worden** in een bestand onder verzegelde omslag neergelegd ter griffie. Gaat het om personen bedoeld in artikel **90octies**, dan wordt ter zake gehandeld zoals bepaald in **dat artikel**.
§ 4. De beschikkingen van de onderzoeksrechter, de verslagen van de officieren van gerechtelijke politie bedoeld in artikel 90quater, § 3, en de processen-verbaal die betrekking hebben op de tenuitvoerlegging van de maatregel, worden uiterlijk na het beëindigen van de maatregel bij het dossier gevoegd.	§ 4. De **machtigingen** van de onderzoeksrechter, de verslagen van de officieren van gerechtelijke politie bedoeld in artikel 90quater, § 3, en de processen-verbaal die betrekking hebben op de tenuitvoerlegging van de maatregel, worden uiterlijk na het beëindigen van de maatregelen bij het dossier gevoegd.

Artikel 90septies	**Artikel 90septies**
De communicatie of telecommunicatie opgevangen als gevolg van de maatregelen die genomen zijn met toepassing van de artikelen 90ter, 90quater en 90quinquies, wordt opgenomen. Het voorwerp van de maatregel en de dagen en uren waarop deze is uitgevoerd, worden opgenomen bij het begin en op het einde van iedere opname die erop betrekking heeft.	**§ 1. De passende middelen worden aangewend om de integriteit en de vertrouwelijkheid van de opgenomen niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem te waarborgen.** **§ 2. Ieder bestand bevat het onderwerp van de opgenomen niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem en de dagen en uren waarop de maatregel is uitgevoerd.**
Iedere aantekening in het kader van de tenuitvoerlegging van de maatregelen bedoeld in het voorgaande lid door de daartoe aangewezen personen, die niet is opgetekend in een proces-verbaal, wordt vernietigd, met uitzondering van de overschrijving van de van belang geachte gedeelten van de opgenomen communicaties of telecommunicaties van de opname, de eventuele vertaling ervan en de vermelding van de aangehaalde onderwerpen en van de identificatiegegevens van de telecommunicatiemiddelen van waaruit of waarnaar opgeroepen werd wat betreft de niet van belang geachte communicaties en telecommunicaties. De voor de uitvoering van de maatregel aangewezen officier van gerechtelijke politie gaat over tot deze vernietiging en vermeldt dit in een proces-verbaal.	**§ 3.** Iedere aantekening in het kader van de tenuitvoerlegging van de maatregelen bedoeld in **de artikelen 90ter, 90quater en 90quinquies** door de daartoe aangewezen personen, die niet is opgetekend in een proces-verbaal, wordt vernietigd, met uitzondering van **het vermelde in artikel 90sexies, §1, 2°, 3° en 4° en onverminderd artikel 33 van de wet van XXX betreffende de verbetering van de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden**. De voor de uitvoering van de maatregel aangewezen **officieren** van gerechtelijke politie **gaan** over tot deze vernietiging en vermelden dit in een proces-verbaal. **Om beheersredenen en om aan de verplichting van artikel 90decies te kunnen voldoen, kunnen de strikt noodzakelijke administratieve gegevens evenwel bewaard blijven bij de dienst aangewezen door de Koning.**
De opnamen worden samen met de overschrijving van de van belang geachte gedeelten van de opgenomen communicaties of telecommunicaties, de eventuele vertaling ervan, de vermelding van de aangehaalde onderwerpen en van de identificatiegegevens van de telecommunicatiemiddelen van waaruit of waarnaar opgeroepen werd wat betreft de niet van belang geachte communicaties en telecommunicaties, en de afschriften van de processen-verbaal onder verzegelde omslag ter griffie bewaard.	**§ 4. De bestanden bedoeld in artikel 90sexies, §1, 1° worden bewaard onder verzegelde omslag ter griffie. Ze kunnen bovendien ook worden bewaard bij de dienst aangewezen door de Koning onder de voorwaarden en modaliteiten door Hem** bepaald na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer. **De stukken bedoeld in artikel 90sexies, §1, 2°, 3° en 4° en de afschriften van de processen-verbaal worden onder**

	verzegelde omslag ter griffie bewaard.
De griffier vermeldt in een per dag bijgehouden, bijzonder register :	**§ 5.** De griffier vermeldt in een per dag bijgehouden, bijzonder register:
1° het neerleggen van iedere opname, alsook van de overschrijving van de van belang geachte gedeelten van de opgenomen communicaties of telecommunicaties, de eventuele vertaling ervan en de vermelding van de aangehaalde onderwerpen en van de identificatiegegevens van de telecommunicatiemiddelen van waaruit of waarnaar opgeroepen werd wat betreft de niet van belang geachte communicaties en telecommunicaties;	1° **de dag** van de neerlegging van de **in artikel 90sexies, §1 bedoelde bestanden en stukken, alsmede van ieder afschrift van proces-verbaal**;
2° het neerleggen van ieder afschrift van procesverbaal;	
3° de dag van de neerlegging ervan;	
4° de naam van de onderzoeksrechter die de maatregel heeft bevolen of bevestigd en het voorwerp ervan;	2° de naam van de onderzoeksrechter die de maatregelen heeft bevolen of bevestigd en het voorwerp ervan;
5° de dag waarop de zegels zijn verbroken en in voorkomend geval opnieuw zijn gelegd;	3° de dag waarop de zegels zijn verbroken en in voorkomend geval opnieuw zijn gelegd;
6° de datum van de kennisname van de opname, de overschrijving van de van belang geachte gedeelten van de opgenomen communicaties of telecommunicaties, de eventuele vertaling ervan en de vermelding van de aangehaalde onderwerpen en van de identificatiegegevens van de telecommunicatiemiddelen van waaruit of waarnaar opgeroepen werd wat betreft de niet van belang geachte communicaties en telecommunicaties of van de afschriften van de processen-verbaal, alsook de naam van de personen die er kennis van genomen hebben;	4° de datum van de kennisname van de **in artikel 90sexies, §1 bedoelde bestanden en stukken,** van de afschriften van processen-verbaal, alsook de namen van de personen er kennis van genomen hebben;
7° iedere andere gebeurtenis die erop betrekking heeft.	5° iedere andere gebeurtenis die erop betrekking heeft.
De passende middelen worden aangewend om de integriteit en de vertrouwelijkheid van de opgenomen communicatie of telecommunicatie te waarborgen, en voor zover mogelijk, de overschrijving of vertaling hiervan tot stand te brengen. Hetzelfde geldt voor de bewaring op de griffie van de	**§6.** De inverdenkinggestelde, de beklaagde, de burgerlijke partij of hun raadsman ontvangen op eenvoudig verzoek een kopie van het geheel van de **opgenomen niet voor het publiek toegankelijke communicaties of gegevens van een**

opnamen en de overschrijving of vertaling hiervan en voor de vermeldingen in het bijzonder register. De Koning bepaalt, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, deze middelen en het ogenblik waarop ze de bewaring onder verzegelde omslag of het bijzonder register, bedoeld in het derde en het vierde lid, vervangen.	**informaticasysteem,** waarvan bepaalde van belang geachte gedeelten overgeschreven **of weergegeven** werden en opgenomen werden in een proces-verbaal waarvan ze inzage hebben.
De inverdenkinggestelde, de beklaagde, de burgerlijke partij, de burgerrechtelijk aansprakelijke partij of hun raadsman ontvangen op eenvoudig verzoek een kopie van het geheel van de opnames van de communicaties en telecommunicaties waarvan bepaalde van belang geachte gedeelten overgeschreven werden en opgenomen werden in een proces-verbaal waarvan ze inzage hebben.	**De inverdenkinggestelde, de beklaagde, de burgerlijke partij of hun raadsman kunnen de rechter verzoeken om de overeenkomstig §4 ter griffie neergelegde andere bestanden of stukken ter griffie te raadplegen, en bijkomende delen van de opgenomen communicatie of gegevens over te schrijven of weer te geven. Het verzoek dat gericht is tot de onderzoeksrechter, wordt behandeld overeenkomstig artikel 61quinquies.**
De rechter spreekt zich uit over het verzoek van de inverdenkinggestelde, de beklaagde, de burgerlijke partij of hun raadsman, om het geheel of gedeelten van de andere ter griffie neergelegde opnamen en overschrijvingen die niet zijn opgetekend in een proces-verbaal, te raadplegen, en over hun verzoek tot overschrijving van bijkomende delen van de opnamen. Het verzoek dat gericht is tot de onderzoeksrechter, wordt behandeld overeenkomstig artikel 61quinquies. De onderzoeksrechter kan dit verzoek bovendien afwijzen om redenen die verband houden met de bescherming van andere rechten of belangen van personen. Onverminderd hetgeen in de vorige leden is bepaald, spreekt de rechter zich uit over het verzoek van de inverdenkinggestelde, de beklaagde, de burgerlijke partij of hun raadsman om de gedeelten van de ter griffie neergelegde opnamen van privécommunicatie of -telecommunicatie waaraan de betrokkene heeft deelgenomen en die niet zijn overgeschreven en opgetekend in een proces-verbaal, te raadplegen, en over hun verzoek tot overschrijving van bijkomende delen van deze opnamen.	**De rechter kan het verzoek afwijzen indien hij de raadpleging of de overschrijving of weergave van bijkomende delen niet noodzakelijk acht om de waarheid aan de dag te brengen, indien hij dit op dat ogenblik nadelig acht voor het onderzoek, of om redenen die verband houden met de bescherming van andere rechten of belangen van personen. Hij kan de raadpleging of de overschrijving of weergave van bijkomende delen ook beperken tot een door hem nader omschreven selectie van bestanden of stukken.**
Artikel 90octies	**Artikel 90octies**

De maatregel kan alleen betrekking hebben op de lokalen aangewend voor beroepsdoeleinden, de woonplaats of de communicatie- of telecommunicatiemiddelen van een advocaat of een arts, indien deze er zelf van verdacht worden een van de strafbare feiten bedoeld in artikel 90ter te hebben gepleegd of eraan deelgenomen te hebben, of, indien precieze feiten doen vermoeden dat derden die ervan verdacht worden een van de strafbare feiten bedoeld in artikel 90ter te hebben gepleegd, gebruik maken van diens lokalen, woonplaats of communicatie- of telecommunicatiemiddelen.	**§1.** De maatregel kan alleen betrekking hebben op de lokalen aangewend voor beroepsdoeleinden, de woonplaats**, de communicatiemiddelen of de informaticasystemen** van een advocaat of een arts, indien deze er zelf van verdacht worden een van de strafbare feiten bedoeld in artikel 90ter te hebben gepleegd of eraan deelgenomen te hebben, of, indien precieze feiten doen vermoeden dat derden die ervan verdacht worden een van de strafbare feiten bedoeld in artikel 90ter te hebben gepleegd, gebruik maken van diens lokalen, woonplaats, **communicatiemiddelen of informaticasystemen.**
De maatregel mag niet ten uitvoer worden gelegd, zonder dat, naar gelang van het geval, de stafhouder of de vertegenwoordiger van de provinciale orde van geneesheren ervan op de hoogte is.	**§2.** De maatregel mag niet ten uitvoer worden gelegd, zonder dat, naar gelang van het geval, de stafhouder of de vertegenwoordiger van de provinciale orde van geneesheren ervan op de hoogte is.
Dezelfden zullen door de onderzoeksrechter in kennis worden gesteld van hetgeen volgens hem als communicatie of telecommunicatie onder het beroepsgeheim valt en niet wordt opgetekend in het proces-verbaal overeenkomstig artikel 90sexies, derde lid.	**Deze personen zijn tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.** **§3. De onderzoeksrechter beoordeelt, na overleg met de stafhouder of de vertegenwoordiger van de provinciale orde van geneesheren, welke gedeelten van de in artikel 90sexies, §3, bedoelde niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem, die hij van belang acht voor het onderzoek, onder het beroepsgeheim vallen en welke niet.** **Enkel de gedeelten van de communicatie of gegevens bedoeld in het vorige lid die worden geacht niet onder het beroepsgeheim te vallen, worden overgeschreven of weergegeven en worden desgevallend vertaald. De onderzoeksrechter laat hiervan proces-verbaal opmaken. De bestanden bevattende deze communicatie of gegevens worden onder verzegelde omslag neergelegd ter griffie.** **Alle overige communicatie of gegevens worden in een ander bestand onder afzonderlijke verzegelde omslag**

	neergelegd ter griffie.
Artikel 90novies	**Artikel 90novies**
Uiterlijk vijftien dagen nadat de beslissing over de regeling van de rechtspleging definitief is geworden of nadat de dagvaarding bedoeld in artikel 524bis , § 6, ter griffie van de rechtbank of het hof werd neergelegd, stelt de griffier, op vordering van de procureur des Konings of in voorkomend geval van de procureur-generaal, iedere persoon ten aanzien van wie een maatregel bedoeld in artikel 90ter is genomen, schriftelijk in kennis van de aard van die maatregel en van de dagen waarop deze is uitgevoerd.	Uiterlijk vijftien dagen nadat de beslissing over de regeling van de rechtspleging definitief is geworden of nadat de dagvaarding bedoeld in artikel 524bis , § 6, ter griffie van de rechtbank of het hof werd neergelegd, stelt de griffier, op vordering van de procureur des Konings of in voorkomend geval van de procureur-generaal, iedere persoon ten aanzien van wie een maatregel bedoeld in artikel 90ter is genomen, schriftelijk in kennis van de aard van die maatregel en van de dagen waarop deze is uitgevoerd, **tenzij diens identiteit of woonplaats redelijkerwijze niet achterhaald kan worden**.
Artikel 90decies	**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. 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	De Minister van Justitie brengt jaarlijks verslag uit aan het Parlement over de toepassing van de artikelen 90ter tot en met 90novies. 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**, 46quinquies**, 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.

dossiers, personen en misdrijven. 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.	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.
Art. 235ter	**Art. 235ter**
§ 1. De kamer van inbeschuldigingstelling is belast met de controle over de toepassing van de bijzondere opsporingsmethoden observatie en infiltratie.	§ 1. De kamer van inbeschuldigingstelling is belast met de controle over de toepassing van de bijzondere opsporingsmethoden observatie en infiltratie**, <u>en over de toepassing van de maatregelen bedoeld in de artikel 46sexies indien daarbij een vertrouwelijk dossier werd aangelegd.</u>**
De kamer van inbeschuldigingstelling onderzoekt, op vordering van het openbaar ministerie, de regelmatigheid van de bijzondere opsporingsmethoden observatie en infiltratie bij het afsluiten van het opsporingsonderzoek waarin deze methoden werden toegepast en alvorens het openbaar ministerie tot rechtstreekse dagvaarding overgaat.	De kamer van inbeschuldigingstelling onderzoekt, op vordering van het openbaar ministerie, de regelmatigheid van de bijzondere opsporingsmethoden observatie en infiltratie **<u>en van de maatregelen bedoeld in artikel 46sexies</u>** bij het afsluiten van het opsporingsonderzoek waarin deze methoden werden toegepast en alvorens het openbaar ministerie tot rechtstreekse dagvaarding overgaat.
De kamer van inbeschuldigingstelling onderzoekt op het ogenblik dat de onderzoeksrechter zijn dossier aan de procureur des Konings overzendt krachtens artikel 127, § 1, eerste lid, op vordering van het openbaar ministerie, de regelmatigheid van de bijzondere opsporingsmethoden observatie en infiltratie die werden toegepast in het kader van het gerechtelijk onderzoek of in het daaraan voorafgaande opsporingsonderzoek.	De kamer van inbeschuldigingstelling onderzoekt op het ogenblik dat de onderzoeksrechter zijn dossier aan de procureur des Konings overzendt krachtens artikel 127, § 1, eerste lid, op vordering van het openbaar ministerie, de regelmatigheid van de bijzondere opsporingsmethoden observatie en infiltratie **<u>en van de maatregelen bedoeld in artikel 46sexies</u>** die werden toegepast in het kader van het gerechtelijk onderzoek of in het daaraan voorafgaande opsporingsonderzoek.
§ 2. De kamer van inbeschuldigingstelling doet uitspraak binnen dertig dagen na ontvangst van de vordering van het openbaar ministerie. Deze termijn wordt teruggebracht tot acht dagen indien één van de inverdenkinggestelden zich in voorlopige hechtenis bevindt.	§ 2. De kamer van inbeschuldigingstelling doet uitspraak binnen dertig dagen na ontvangst van de vordering van het openbaar ministerie. Deze termijn wordt teruggebracht tot acht dagen indien één van de inverdenkinggestelden zich in voorlopige hechtenis bevindt.
De kamer van inbeschuldigingstelling hoort, afzonderlijk en buiten de aanwezigheid van de partijen, de opmerkingen van de procureur-generaal.	De kamer van inbeschuldigingstelling hoort, afzonderlijk en buiten de aanwezigheid van de partijen, de opmerkingen van de procureur-generaal.

Zij hoort, in aanwezigheid van de procureur-generaal, afzonderlijk de burgerlijke partijen en de inverdenkinggestelden, na kennisgeving die hen door de griffier ten laatste achtenveertig uur vóór de zitting per faxpost of bij een ter post aangetekende brief wordt gedaan. De griffier stelt hen in dezelfde post eveneens ter kennis dat het strafdossier tijdens deze periode op de griffie in origineel of in kopie ter inzage ligt.[De kamer van inbeschuldigingstelling kan beslissen dat de inverdenkinggestelde die zich in voorlopige hechtenis bevindt in een videoconferentie verschijnt.]	Zij hoort, in aanwezigheid van de procureur-generaal, afzonderlijk de burgerlijke partijen en de inverdenkinggestelden, na kennisgeving die hen door de griffier ten laatste achtenveertig uur vóór de zitting per faxpost of bij een ter post aangetekende brief wordt gedaan. De griffier stelt hen in dezelfde post eveneens ter kennis dat het strafdossier tijdens deze periode op de griffie in origineel of in kopie ter inzage ligt. .[De kamer van inbeschuldigingstelling kan beslissen dat de inverdenkinggestelde die zich in voorlopige hechtenis bevindt in een videoconferentie verschijnt.]
Zij kan, met betrekking tot de toegepaste bijzondere opsporingsmethoden observatie en infiltratie, de onderzoeksrechter en de in de artikelen 47sexies, § 3, 6° en 47octies, § 3, 6° bedoelde officier van gerechtelijke politie afzonderlijk en buiten de aanwezigheid van de partijen horen.	Zij kan, met betrekking tot de toegepaste bijzondere opsporingsmethoden observatie en infiltratie **en de maatregelen bedoeld in artikel 46sexies**, de onderzoeksrechter, de in de artikelen 47sexies, § 3, 6° en 47octies, § 3, 6° bedoelde officier van gerechtelijke politie, **en de officier van gerechtelijke politie belast met de leiding over de uitvoering van de maatregelen bedoeld in artikel 46sexies** afzonderlijk en buiten de aanwezigheid van de partijen horen.
De kamer van inbeschuldigingstelling kan de onderzoeksrechter gelasten de politieambtenaren die belast zijn met de uitvoering van de observatie en infiltratie en de in artikel 47octies, § 1, tweede lid, bedoelde burger te horen met toepassing van de artikelen 86bis en 86ter. Zij kan beslissen bij het verhoor door de onderzoeksrechter aanwezig te zijn of één van haar leden daartoe af te vaardigen.	De kamer van inbeschuldigingstelling kan de onderzoeksrechter gelasten de politieambtenaren die belast zijn met de uitvoering van de observatie en infiltratie, ~~en~~ de in artikel 47octies, § 1, tweede lid, bedoelde burger, **de politieambtenaren belast met de uitvoering van de maatregelen bedoeld in 46sexies, en de in artikel 46sexies, § 1, tweede lid bedoelde burger** te horen met toepassing van de artikelen 86bis en 86ter. Zij kan beslissen bij het verhoor door de onderzoeksrechter aanwezig te zijn of één van haar leden daartoe af te vaardigen.
§ 3. Het openbaar ministerie legt aan de voorzitter van de kamer van inbeschuldigingstelling het vertrouwelijk dossier voor bedoeld in de artikelen 47septies, § 1, tweede lid, of 47novies, § 1, tweede lid, dat betrekking heeft op het opsporingsonderzoek of gerechtelijk onderzoek bedoeld in § 1. Enkel de magistraten van de kamer van inbeschuldigingstelling hebben het recht dit vertrouwelijk dossier in te zien.	§ 3. Het openbaar ministerie legt aan de voorzitter van de kamer van inbeschuldigingstelling het vertrouwelijk dossier voor bedoeld in de artikelen **46sexies, §3, zevende lid,** 47septies, § 1, tweede lid, of 47novies, § 1, tweede lid, dat betrekking heeft op het opsporingsonderzoek of gerechtelijk onderzoek bedoeld in § 1. Enkel de magistraten van de kamer van inbeschuldigingstelling hebben het recht dit vertrouwelijk dossier in te zien.

De voorzitter van de kamer van inbeschuldigingstelling neemt de nodige maatregelen ter beveiliging van het vertrouwelijk dossier. Hij bezorgt het vertrouwelijk dossier, na kennisname ervan, onmiddellijk aan het openbaar ministerie terug.	De voorzitter van de kamer van inbeschuldigingstelling neemt de nodige maatregelen ter beveiliging van het vertrouwelijk dossier. Hij bezorgt het vertrouwelijk dossier, na kennisname ervan, onmiddellijk aan het openbaar ministerie terug.
§ 4. In het arrest van de kamer van inbeschuldigingstelling mag geen gewag worden gemaakt van de inhoud van het vertrouwelijk dossier, noch van enig element dat de afscherming van de gebruikte technische hulpmiddelen en de politionele onderzoekstechnieken of de vrijwaring van de veiligheid en de afscherming van de identiteit van de informant, de politieambtenaren die belast zijn met de uitvoering van de observatie of infiltratie en de in artikel 47octies, § 1, tweede lid, bedoelde burger in het gedrang kan brengen.	§ 4. In het arrest van de kamer van inbeschuldigingstelling mag geen gewag worden gemaakt van de inhoud van het vertrouwelijk dossier, noch van enig element dat de afscherming van de gebruikte technische hulpmiddelen en de politionele onderzoekstechnieken of de vrijwaring van de veiligheid en de afscherming van de identiteit van de informant, de politieambtenaren die belast zijn met de uitvoering van de observatie of infiltratie, ~~en~~ de in artikel 47octies, § 1, tweede lid, bedoelde burger, de politieambtenaren die belast zijn met de uitvoering van de observatie, **de** infiltratie **of de maatregel bedoeld in artikel 46sexies,** en de in **de** artikel**en** 47octies, §1, tweede lid **en 46sexies, §1, tweede lid** bedoelde burger in het gedrang kan brengen.
§ 5. Er wordt verder gehandeld overeenkomstig artikel 235bis, §§ 5 en 6.	§ 5. Er wordt verder gehandeld overeenkomstig artikel 235bis, §§ 5 en 6.
Artikel 235quater	**Artikel 235quater**
§ 1. Onverminderd de uitoefening van de controle bedoeld in artikel 235ter, kan de kamer van inbeschuldigingstelling voorlopig, ambtshalve, op verzoek van de onderzoeksrechter of op vordering van het openbaar ministerie, tijdens het gerechtelijk onderzoek, de regelmatigheid onderzoeken van de bijzondere opsporingsmethoden observatie en infiltratie die werden toegepast in het kader van dit gerechtelijk onderzoek of in het daaraan voorafgaande opsporingsonderzoek.	§ 1. Onverminderd de uitoefening van de controle bedoeld in artikel 235ter, kan de kamer van inbeschuldigingstelling voorlopig, ambtshalve, op verzoek van de onderzoeksrechter of op vordering van het openbaar ministerie, tijdens het gerechtelijk onderzoek, de regelmatigheid onderzoeken van de bijzondere opsporingsmethoden observatie en infiltratie **en van de maatregel bedoeld in artikel 46sexies indien daarbij een vertrouwelijk dossier werd aangelegd,** die werden toegepast in het kader van dit gerechtelijk onderzoek of in het daaraan voorafgaande opsporingsonderzoek.
Opdat de kamer van inbeschuldigingstelling haar controle ambtshalve zou kunnen uitoefenen, informeren de procureurs des Konings van haar rechtsgebied systematisch	Opdat de kamer van inbeschuldigingstelling haar controle ambtshalve zou kunnen uitoefenen, informeren de procureurs des Konings van haar rechtsgebied systematisch

en onmiddellijk de voorzitter van de kamer van inbeschuldigingstelling over de dossiers waarvoor tot observaties en infiltraties werd beslist door het openbaar ministerie of door de onderzoeksrechter.	en onmiddellijk de voorzitter van de kamer van inbeschuldigingstelling over de dossiers waarvoor **door het openbaar ministerie of door de onderzoeksrechter werd beslist** tot observaties en infiltraties **en tot de maatregel bedoeld in artikel 46sexies indien daarbij een vertrouwelijk dossier werd aangelegd**.
§ 2. De kamer van inbeschuldigingstelling hoort, afzonderlijk en buiten de aanwezigheid van de partijen, de opmerkingen van de procureur-generaal.	§ 2. De kamer van inbeschuldigingstelling hoort, afzonderlijk en buiten de aanwezigheid van de partijen, de opmerkingen van de procureur-generaal.
Zij kan, met betrekking tot de toegepaste bijzondere opsporingsmethoden observatie of infiltratie, de onderzoeksrechter en de in de artikelen 47sexies, § 3, 6°, en 47octies, § 3, 6°, bedoelde officier van gerechtelijke politie afzonderlijk en buiten de aanwezigheid van de partijen horen.	Zij kan, met betrekking tot de toegepaste bijzondere opsporingsmethoden observatie of infiltratie **en de maatregel bedoeld in artikel 46sexies,** de onderzoeksrechter, de in de artikelen 47sexies, § 3, 6°, en 47octies, § 3, 6°, bedoelde officier van gerechtelijke politie **en de officier van gerechtelijke politie belast met de leiding over de uitvoering van de maatregel bedoeld in artikel 46sexies** afzonderlijk en buiten de aanwezigheid van de partijen horen.
§ 3. Het openbaar ministerie legt aan de voorzitter van de kamer van inbeschuldigingstelling het vertrouwelijk dossier voor bedoeld in de artikelen 47septies, § 1, tweede lid, of 47novies, § 1, tweede lid, dat betrekking heeft op het gerechtelijk onderzoek bedoeld in § 1. Enkel de magistraten van de kamer van inbeschuldigingstelling hebben het recht dit vertrouwelijk dossier in te zien.	§ 3. Het openbaar ministerie legt aan de voorzitter van de kamer van inbeschuldigingstelling het vertrouwelijk dossier voor bedoeld in de artikelen 47septies, § 1, tweede lid, of 47novies, § 1, tweede lid **of 46sexies, § 3, zevende lid,** dat betrekking heeft op het gerechtelijk onderzoek bedoeld in § 1. Enkel de magistraten van de kamer van inbeschuldigingstelling hebben het recht dit vertrouwelijk dossier in te zien.
De voorzitter van de kamer van inbeschuldigingstelling neemt de nodige maatregelen ter beveiliging van het vertrouwelijk dossier. Hij bezorgt het vertrouwelijk dossier, na kennisname ervan, onmiddellijk aan het openbaar ministerie terug.	De voorzitter van de kamer van inbeschuldigingstelling neemt de nodige maatregelen ter beveiliging van het vertrouwelijk dossier. Hij bezorgt het vertrouwelijk dossier, na kennisname ervan, onmiddellijk aan het openbaar ministerie terug.
§ 4. In het arrest van de kamer van inbeschuldigingstelling mag geen gewag worden gemaakt van de inhoud van het vertrouwelijk dossier, noch van enig element dat de afscherming van de gebruikte technische hulpmiddelen en de politionele onderzoekstechnieken of de vrijwaring van de veiligheid en de afscherming van de identiteit van de informant, de	§ 4. In het arrest van de kamer van inbeschuldigingstelling mag geen gewag worden gemaakt van de inhoud van het vertrouwelijk dossier, noch van enig element dat de afscherming van de gebruikte technische hulpmiddelen en de politionele onderzoekstechnieken of de vrijwaring van de veiligheid en de afscherming van de identiteit van de informant, de

politieambtenaren die belast zijn met de uitvoering van de observatie of infiltratie en de in artikel 47octies, § 1, tweede lid, bedoelde burger in het gedrang kan brengen.	politieambtenaren die belast zijn met de uitvoering van de observatie**, de** infiltratie **of de maatregel bedoeld in artikel 46sexies, en** de in **de** artikel**en** 47octies, § 1, tweede lid **en 46sexies, § 1, tweede lid** bedoelde burger in het gedrang kan brengen.
Artikel 464/13	**Artikel 464/13**
§ 1. De SUO-magistraat of de gevorderde politiedienst kan bij een schriftelijke en met redenen omklede beslissing, van de operator van een elektronisch communicatienetwerk of van de verstrekker van een elektronische communicatiedienst de mededeling van de volgende inlichtingen vorderen :	§ 1. De SUO-magistraat of de gevorderde politiedienst kan bij een schriftelijke en met redenen omklede beslissing, van de **actoren bedoeld in het tweede lid** de mededeling van de volgende inlichtingen vorderen :
1° de identificatie van een abonnee of een gewoonlijke gebruiker van een elektronische communicatiedienst of van het gebruikte elektronische communicatiemiddel;	1° de identificatie van een abonnee of een gewoonlijke gebruiker van een **dienst zoals bedoeld in het tweede lid, tweede streepje,** of van het gebruikte elektronische communicatiemiddel;
2° de identificatie van de elektronische communicatiediensten waarop een bepaalde persoon geabonneerd is of die door een bepaalde persoon gewoonlijk worden gebruikt.	2° de identificatie van de **diensten zoals bedoeld in het tweede lid, tweede streepje,** waarop een bepaalde persoon geabonneerd is of die door een bepaalde persoon gewoonlijk worden gebruikt. **De volgende actoren zijn gehouden tot medewerking overeenkomstig het vorige lid:** **- de operator van een elektronisch communicatienetwerk; en** **- iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.**
§ 2. Iedere operator van een elektronisch communicatienetwerk en iedere verstrekker van een elektronische communicatiedienst verstrekt alle beschikbare inlichtingen binnen de termijn en op de wijze die bepaald	§ 2. **De actoren bedoeld in § 1, tweede lid, verstrekken** alle beschikbare inlichtingen **in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de beslissing, volgens de modaliteiten** die bepaald

worden bij het ter uitvoering van artikel 46bis, § 2, eerste en tweede lid, genomen koninklijk besluit. Weigering om de gegevens mee te delen, wordt gestraft met geldboete van zesentwintig euro tot tienduizend euro. § 3. Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.]1	worden bij het ter uitvoering van artikel 46bis, § 2, eerste en tweede lid, genomen koninklijk besluit. **Iedere persoon die de gegevens weigert mee te delen of deze niet meedeelt in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de beslissing,** wordt gestraft met geldboete van zesentwintig euro tot tienduizend euro. § 3. Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.
Artikel 464/25	**Artikel 464/25**
§ 1. De SUO-magistraat of de gevorderde politiedienst kan een operator van een elektronisch communicatienetwerk of de verstrekker van een elektronische communicatiedienst vorderen om : 1° de oproepgegevens te doen opsporen van elektronische communicatiemiddelen waaruit of waarnaar oproepen worden of werden gedaan; 2° de oorsprong of de bestemming van elektronische communicaties te laten lokaliseren.	§ 1. De SUO-magistraat of de gevorderde politiedienst kan **de actoren bedoeld in het tweede lid** vorderen om : 1° de oproepgegevens te doen opsporen van elektronische communicatiemiddelen waaruit of waarnaar oproepen worden of werden gedaan; 2° de oorsprong of de bestemming van elektronische communicaties te laten lokaliseren. **De volgende actoren zijn gehouden tot medewerking overeenkomstig het vorige lid:** **- de operator van een elektronisch communicatienetwerk; en** **- iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder wordt ook de**

	verstrekker van een elektronische communicatiedienst begrepen.
In de in het eerste lid bedoelde gevallen worden voor ieder elektronisch communicatiemiddel waarvoor de oproep-gegevens worden opgespoord of waarvan de oorsprong of de bestemming van de elektronische communicaties 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 in het eerste lid bedoelde gevallen worden voor ieder elektronisch communicatiemiddel waarvoor de oproep-gegevens worden opgespoord of waarvan de oorsprong of de bestemming van de elektronische communicaties wordt gelokaliseerd, de dag, het uur, de duur en, indien nodig, de plaats van de oproep vastgesteld en opgenomen in een proces-verbaal.
De SUO-magistraat vermeldt in zijn beslissing de duur van de maatregel, die, wat de toekomstige elektronische communicatiegegevens betreft, niet langer kan zijn dan twee maanden te rekenen vanaf het bevelschrift, behoudens een hernieuwing.	De SUO-magistraat vermeldt in zijn beslissing de duur van de maatregel, die, wat de toekomstige elektronische communicatiegegevens betreft, niet langer kan zijn dan twee maanden te rekenen vanaf het bevelschrift, behoudens een hernieuwing.
§ 2. Iedere operator van een elektronische communicatiedienst en iedere verstrekker van een elektronische communicatiedienst delen de gevorderde inlichtingen mee binnen de termijn en volgens de bij het ter uitvoering van artikel 88bis, § 2, eerste en derde lid, genomen koninklijk besluit bepaalde nadere regels.	§ 2. **De actoren bedoeld in § 1, tweede lid** delen de gevorderde inlichtingen mee **in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de beslissing, volgens de modaliteiten die bepaald worden** bij het ter uitvoering van artikel 88bis, § 2, eerste en derde lid, genomen koninklijk besluit.
Iedere persoon die zijn technische medewerking weigert aan de in dit artikel bedoelde vorderingen wordt gestraft met een geldboete van zesentwintig euro tot tienduizend euro.	Iedere persoon die zijn technische medewerking aan de in dit artikel bedoelde vorderingen **weigert of niet verleent in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de beslissing,** wordt gestraft met een geldboete van zesentwintig euro tot tienduizend euro.
§ 3. Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht.	§ 3. Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht.
Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.	Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.
STRAFWETBOEK	**STRAFWETBOEK**
Boek 2, Titel VI, Hoofstuk Vbis – Afluisteren, kennisnemen en opnemen	**Boek 2, Titel VI, Hoofstuk Vbis – Onderscheppen, kennisnemen en**

van privé-communicatie en -telecommunicatie.	**opnemen van niet voor het publiek toegankelijke communicatie en gegevens van een informaticasysteem**
Art. 259bis	**Art. 259bis**
§ 1. Met gevangenisstraf van zes maanden tot twee jaar en met geldboete van vijfhonderd [euro] tot twintigduizend [euro] of met een van die straffen alleen wordt gestraft ieder openbaar officier of ambtenaar, drager of agent van de openbare macht die, naar aanleiding van de uitoefening van zijn bediening, buiten de gevallen die de wet bepaalt of zonder inachtneming van de vormen die zij voorschrijft:	§ 1. Met gevangenisstraf van zes maanden tot twee jaar en met geldboete van vijfhonderd [euro] tot twintigduizend [euro] of met een van die straffen alleen wordt gestraft ieder openbaar officier of ambtenaar, drager of agent van de openbare macht die, naar aanleiding van de uitoefening van zijn bediening, buiten de gevallen die de wet bepaalt of zonder inachtneming van de vormen die zij voorschrijft:
1° ofwel, opzettelijk, met behulp van enig toestel privé-communicatie of -telecommunicatie, waaraan hij niet deelneemt, tijdens de overbrenging ervan, afluistert of doet afluisteren, er kennis van neemt of doet van nemen, opneemt of doet opnemen, zonder de toestemming van alle deelnemers aan die communicatie of telecommunicatie;	1° ofwel, opzettelijk, met behulp van enig toestel **niet voor publiek toegankelijke communicatie**, waaraan hij niet deelneemt, **onderschept of doet onderscheppen**, er kennis van neemt of doet van nemen, opneemt of doet opnemen, zonder de toestemming van alle deelnemers aan die **communicatie**;
2° ofwel, met het opzet een van de hierboven omschreven misdrijven te plegen, enig toestel opstelt of doet opstellen;	2° ofwel, met het opzet een van de hierboven omschreven misdrijven te plegen, enig toestel opstelt of doet opstellen;
3° ofwel, wetens, de inhoud van privé-communicatie of -telecommunicatie die onwettig afgeluisterd of opgenomen is of waarvan onwettig kennis genomen is, onder zich houdt, aan een andere persoon onthult of verspreidt, of wetens enig gebruik maakt van een op die manier verkregen inlichting.	3° ofwel, wetens, **de inhoud van niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem die onwettig onderschept of opgenomen zijn** of waarvan onwettig kennis genomen is, onder zich houdt, aan een andere persoon onthult of verspreidt, of wetens enig gebruik maakt van een op die manier verkregen inlichting.
§ 2. Met gevangenisstraf van zes maanden tot drie jaar en met geldboete van vijfhonderd [euro] tot dertigduizend [euro] of met een van die straffen alleen wordt gestraft ieder openbaar officier of ambtenaar, drager of agent van de openbare macht die, naar aanleiding van de uitoefening van zijn bediening, buiten de gevallen die de wet bepaalt of zonder inachtneming van de vormen die zij voorschrijft, met bedrieglijk opzet of met het oogmerk te schaden, gebruik maakt van een wettig gemaakte opname van privé-communicatie of -	§ 2. Met gevangenisstraf van zes maanden tot drie jaar en met geldboete van vijfhonderd [euro] tot dertigduizend [euro] of met een van die straffen alleen wordt gestraft ieder openbaar officier of ambtenaar, drager of agent van de openbare macht die, naar aanleiding van de uitoefening van zijn bediening, buiten de gevallen die de wet bepaalt of zonder inachtneming van de vormen die zij voorschrijft, met bedrieglijk opzet of met het oogmerk te schaden, gebruik maakt van **een wettig gemaakte opname van niet voor publiek**

telecommunicatie.	**<u>toegankelijke communicatie of gegevens van een informaticasysteem</u>**.
§ 2bis. Met gevangenisstraf van zes maanden tot twee jaar en met geldboete van vijfhonderd euro tot twintigduizend euro of met één van die straffen alleen wordt gestraft ieder openbaar officier of ambtenaar, drager of agent van de openbare macht die, naar aanleiding van de uitoefening van zijn bediening, buiten de gevallen die de wet bepaalt of zonder inachtneming van de vormen die zij voorschrijft, onrechtmatig, een instrument, met inbegrip van informaticagegevens, dat hoofdzakelijk is ontworpen of aangepast om het in § 1 bedoelde misdrijf mogelijk te maken, bezit, produceert, verkoopt, verkrijgt met het oog op het gebruik ervan, invoert, verspreidt of op enige andere manier ter beschikking stelt.	§ 2bis. Met gevangenisstraf van zes maanden tot twee jaar en met geldboete van vijfhonderd euro tot twintigduizend euro of met één van die straffen alleen wordt gestraft ieder openbaar officier of ambtenaar, drager of agent van de openbare macht die, naar aanleiding van de uitoefening van zijn bediening, buiten de gevallen die de wet bepaalt of zonder inachtneming van de vormen die zij voorschrijft, onrechtmatig, een instrument, met inbegrip van informaticagegevens, dat hoofdzakelijk is ontworpen of aangepast om het in § 1 bedoelde misdrijf mogelijk te maken, bezit, produceert, verkoopt, verkrijgt met het oog op het gebruik ervan, invoert, verspreidt of op enige andere manier ter beschikking stelt.
§ 3. Poging tot het plegen van een der misdrijven bedoeld in §§ 1, 2 of 2bis wordt gestraft zoals het misdrijf zelf.	§ 3. Poging tot het plegen van een der misdrijven bedoeld in §§ 1, 2 of 2bis wordt gestraft zoals het misdrijf zelf.
§ 4. De straffen gesteld [in de §§ 1 tot 3] worden verdubbeld indien een overtreding van een van die bepalingen wordt begaan binnen vijf jaar na de uitspraak van een vonnis of een arrest houdende veroordeling wegens een van die strafbare feiten of wegens een van de strafbare feiten beoogd [in artikel 314bis, §§ 1 tot 3], dat in kracht van gewijsde is gegaan.	§ 4. De straffen gesteld [in de §§ 1 tot 3] worden verdubbeld indien een overtreding van een van die bepalingen wordt begaan binnen vijf jaar na de uitspraak van een vonnis of een arrest houdende veroordeling wegens een van die strafbare feiten of wegens een van de strafbare feiten beoogd [in artikel 314bis, §§ 1 tot 3], dat in kracht van gewijsde is gegaan.
§ 5. De bepalingen van § 1, 1° en 2°, zijn niet van toepassing op het zoeken, het onderscheppen, het afluisteren, het kennisnemen of het opnemen door de Algemene Dienst inlichting en Veiligheid van de Krijgsmacht van elke vorm van communicatie uitgezonden in het buitenland zowel om redenen van militaire aard in het kader van de opdrachten gedefinieerd in artikel 11, § 2, 1° en 2°van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst als om redenen van veiligheid en bescherming van onze troepen en van deze van onze geallieerden tijdens opdrachten in het buitenland en van onze onderdanen die in het buitenland gevestigd zijn, zoals gedefinieerd in hetzelfde artikel 11, § 2, 3° et 4°.	§ 5. De bepalingen van § 1, 1° en 2°, zijn niet van toepassing op het zoeken, het onderscheppen, het afluisteren, het kennisnemen of het opnemen door de Algemene Dienst inlichting en Veiligheid van de Krijgsmacht van elke vorm van communicatie uitgezonden in het buitenland zowel om redenen van militaire aard in het kader van de opdrachten gedefinieerd in artikel 11, § 2, 1° en 2°van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst als om redenen van veiligheid en bescherming van onze troepen en van deze van onze geallieerden tijdens opdrachten in het buitenland en van onze onderdanen die in het buitenland gevestigd zijn, zoals gedefinieerd in hetzelfde artikel 11, § 2, 3° et 4°.

Boek 2, Titel VI, Hoofstuk VIIIbis – Misdrijven betreffende het geheim van privé-communicatie en -telecommunicatie.	**Boek 2, Titel VI, Hoofstuk VIIIbis – <u>Midrijven betreffende het geheim van niet voor het publiek toegankelijke communicatie en gegevens van een informaticasysteem</u>**
Art. 341bis	**Art. 341bis**
§ 1. Met gevangenisstraf van zes maanden tot één jaar en met geldboete van tweehonderd [euro] tot tienduizend [euro] of met een van die straffen alleen wordt gestraft hij die:	§ 1. Met gevangenisstraf van zes maanden tot één jaar en met geldboete van tweehonderd [euro] tot tienduizend [euro] of met een van die straffen alleen wordt gestraft hij die:
1° ofwel, opzettelijk, met behulp van enig toestel privé-communicatie of -telecommunicatie, waaraan hij niet deelneemt, tijdens de overbrenging ervan, afluistert of doet afluisteren, er kennis van neemt of doet van nemen, opneemt of doet opnemen, zonder de toestemming van alle deelnemers aan die communicatie of telecommunicatie;	1° ofwel, opzettelijk, met behulp van enig toestel **<u>niet voor publiek toegankelijke communicatie</u>**, waaraan hij niet deelneemt, **<u>onderschept of doet onderscheppen</u>**, er kennis van neemt of doet van nemen, opneemt of doet opnemen, zonder de toestemming van alle deelnemers aan die **<u>communicatie;</u>**
2° ofwel, met het opzet een van de hierboven omschreven misdrijven te plegen, enig toestel opstelt of doet opstellen.	2° ofwel, met het opzet een van de hierboven omschreven misdrijven te plegen, enig toestel opstelt of doet opstellen.
§ 2. Met gevangenisstraf van zes maanden tot twee jaar en met geldboete van vijfhonderd [euro] tot twintigduizend [euro] of met een van die straffen alleen wordt gestraft hij, die wetens, de inhoud van privé-communicatie of -telecommunicatie die onwettig afgeluisterd of opgenomen is of waarvan onwettig kennis genomen is, onder zich houdt, aan een andere persoon onthult of verspreidt, of wetens enig gebruik maakt van een op die manier verkregen inlichting.	§ 2. Met gevangenisstraf van zes maanden tot twee jaar en met geldboete van vijfhonderd [euro] tot twintigduizend [euro] of met een van die straffen alleen wordt gestraft hij, die wetens, **<u>de inhoud van niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem die onwettig onderschept of opgenomen zijn</u>** of waarvan onwettig kennis genomen is, onder zich houdt, aan een andere persoon onthult of verspreidt, of wetens enig gebruik maakt van een op die manier verkregen inlichting.
Met dezelfde straffen wordt gestraft hij die, met bedrieglijk opzet of met het oogmerk te schaden, gebruik maakt van een wettig gemaakte opname van privé-communicatie of -telecommunicatie.	Met dezelfde straffen wordt gestraft hij die, met bedrieglijk opzet of met het oogmerk te schaden, gebruik maakt van **<u>een wettig gemaakte opname van niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem.</u>**
§ 2bis. Met gevangenisstraf van zes maanden tot één jaar en met geldboete van tweehonderd euro tot tienduizend euro of met één van die straffen alleen wordt gestraft hij die, onrechtmatig, een instrument, met	§ 2bis. Met gevangenisstraf van zes maanden tot één jaar en met geldboete van tweehonderd euro tot tienduizend euro of met één van die straffen alleen wordt gestraft hij die, onrechtmatig, een instrument, met

inbegrip van informaticagegevens, dat hoofdzakelijk is ontworpen of aangepast om het in § 1 bedoelde misdrijf mogelijk te maken, bezit, produceert, verkoopt, verkrijgt met het oog op het gebruik ervan, invoert, verspreidt of op enige andere manier ter beschikking stelt. § 3. Poging tot het plegen van een der misdrijven bedoeld in de §§ 1, 2 of 2bis wordt gestraft zoals het misdrijf zelf. § 4. De straffen gesteld in de §§ 1 tot 3 worden verdubbeld indien een overtreding van een van die bepalingen wordt begaan binnen vijf jaar na de uitspraak van een vonnis of een arrest houdende veroordeling wegens een van die strafbare feiten of wegens een van de strafbare feiten beoogd in artikel 259bis, §§ 1 tot 3, dat in kracht van gewijsde is gegaan.	inbegrip van informaticagegevens, dat hoofdzakelijk is ontworpen of aangepast om het in § 1 bedoelde misdrijf mogelijk te maken, bezit, produceert, verkoopt, verkrijgt met het oog op het gebruik ervan, invoert, verspreidt of op enige andere manier ter beschikking stelt. § 3. Poging tot het plegen van een der misdrijven bedoeld in de §§ 1, 2 of 2bis wordt gestraft zoals het misdrijf zelf. § 4. De straffen gesteld in de §§ 1 tot 3 worden verdubbeld indien een overtreding van een van die bepalingen wordt begaan binnen vijf jaar na de uitspraak van een vonnis of een arrest houdende veroordeling wegens een van die strafbare feiten of wegens een van de strafbare feiten beoogd in artikel 259bis, §§ 1 tot 3, dat in kracht van gewijsde is gegaan.
	GEGEVENSBANK STEMAFDRUKKEN
	Art. 33
	De technische gegevens die het mogelijk maken de stem te herkennen van de personen, die het voorwerp uitmaken of hebben uitgemaakt van een maatregel tot interceptie bedoeld in artikel 90ter, §1, van het Wetboek van Strafvordering en die bedoeld worden in artikel 44/5, § 3, 1° van de wet van 5 augustus 1992 op het politieambt, worden gedurende ten hoogste 10 jaar bewaard in de Algemene Nationale Gegevensbank bedoeld in dezelfde wet, met het oog op de identificatie van die personen in het kader van afluisterdossiers uitgevoerd op verzoek van de gerechtelijke overheden. **Behalve die technische gegevens bevat deze gegevensbank ook de gegevens over het dossiernummer, de bevoegde magistraat en het bedoelde gerechtelijke arrondissement.** **De in het eerste lid bedoelde technische gegevens verschillen van de opnames die worden gemaakt in het kader van de tenuitvoerlegging van de maatregel bedoeld in artikel 90ter van het Wetboek van Strafvordering. Die opnames worden**

	niet beoogd door dit artikel. **De doeleinden en nadere regels voor de verwerking van die gegevens worden bepaald in de artikelen 44/7 tot 44/11/1 van de wet van 5 augustus 1992 op het politieambt.**

	TEXTE DE BASE ADAPTÉ AU PROJET DE LOI RELATIVE À L'AMÉLIORATION DES MÉTHODES PARTICULIÈRES DE RECHERCHE ET DE CERTAINES MESURES D'ENQUÊTE CONCERNANT INTERNET, LES COMMUNICATIONS ÉLECTRONIQUES ET LES TÉLÉCOMMUNICATIONS
CODE D'INSTRUCTION CRIMINELLE	**CODE D'INSTRUCTION CRIMINELLE**
Article 39bis	**Article 39bis**
§ 1er. Sans préjudice des dispositions spécifiques de cet article, les règles de ce code relatives à la saisie, y compris l'article 28sexies, sont applicables aux mesures consistant à copier, rendre inaccessibles et retirer des données stockées dans un système informatique.	§ 1er. Sans préjudice des dispositions spécifiques de cet article, les règles de ce code relatives à la saisie, y compris l'article 28sexies, sont applicables aux mesures consistant à copier, rendre inaccessibles et retirer des données stockées dans un système informatique **ou une partie de celui-ci**. § 2. **La recherche dans un système informatique ou une partie de celui-ci qui a été saisi, peut être décidée par un officier de police judiciaire.** **Sans préjudice de l'alinéa précédent, le procureur du Roi peut ordonner une recherche dans un système informatique ou une partie de celui-ci qui peut être saisi par lui.** **Les recherches visées aux alinéas 1 et 2 peuvent uniquement s'étendre aux données sauvegardées dans un système informatique qui est soit saisi, soit susceptible d'être saisi.**
§ 2. Lorsque le procureur du Roi ou l'auditeur du travail découvre dans un système informatique des données stockées qui sont utiles pour les mêmes finalités que celles prévues pour la saisie, mais que la saisie du support n'est néanmoins pas souhaitable, ces données, de même que les données nécessaires pour les comprendre, sont copiées sur des supports qui appartiennent à l'autorité. En cas d'urgence ou pour des raisons techniques, il peut être fait usage de supports qui sont disponibles	(cf. §6, alinéa 1)

pour des personnes autorisées à utiliser le système informatique.	
§ 3. Il utilise en outre les moyens techniques appropriés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité.	(cf. §6, alinéa 2)
Si les données forment l'objet de l'infraction ou ont été produites par l'infraction et si elles sont contraires à l'ordre public ou aux bonnes moeurs ou constituent un danger pour l'intégrité des systèmes informatiques ou pour des données stockées, traitées ou transmises par le biais de tels systèmes, le procureur du Roi [1 ou l'auditeur du travail]1 utilise tous les moyens techniques appropriés pour rendre ces données inaccessibles.	(cf. §6, alinéa 4)
Il peut cependant, sauf dans le cas prévu à l'alinéa précédent, autoriser l'usage ultérieur de l'ensemble ou d'une partie de ces données, lorsque cela ne présente pas de danger pour l'exercice des poursuites.	(cf. §6, alinéa 5)
§ 4. Lorsque la mesure prévue au § 2 n'est pas possible, pour des raisons techniques ou à cause du volume des données, le procureur du Roi utilise les moyens techniques appropriés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité.	(cf. §6, alinéa 3)
(Article 88ter) § 1er. Lorsque le juge d'instruction ordonne une recherche dans un système informatique ou une partie de celui-ci, cette recherche peut être étendue vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée :	§ 3. **Le procureur du Roi peut étendre** la recherche dans un système informatique ou une partie de celui-ci**, entamée sur la base du § 2,** vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée :
- si cette extension est nécessaire pour la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche, et	- si cette extension est nécessaire pour la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche ; et

- si d'autres mesures seraient disproportionnées, ou s'il existe un risque que, sans cette extension, des éléments de preuve soient perdus.	- si d'autres mesures seraient disproportionnées, ou s'il existe un risque que, sans cette extension, des éléments de preuve soient perdus.
§ 2. L'extension de la recherche dans un système informatique ne peut pas excéder les systèmes informatiques ou les parties de tels systèmes auxquels les personnes autorisées à utiliser le système informatique qui fait l'objet de la mesure ont spécifiquement accès.	L'extension de la recherche dans un système informatique ne peut pas excéder les systèmes informatiques ou les parties de tels systèmes auxquels les personnes autorisées à utiliser le système informatique qui fait l'objet de la mesure ont spécifiquement accès.
§ 3. En ce qui concerne les données recueillies par l'extension de la recherche dans un système informatique, qui sont utiles pour les mêmes finalités que celles prévues pour la saisie, les règles prévues à l'article 39bis s'appliquent. Le juge d'instruction informe le responsable du système informatique, sauf si son identité ou son adresse ne peuvent être raisonnablement retrouvées.	En ce qui concerne les données recueillies par l'extension de la recherche dans un système informatique, qui sont utiles pour les mêmes finalités que celles prévues pour la saisie, les règles prévues **au § 6** s'appliquent.
Lorsqu'il s'avère que ces données ne se trouvent pas sur le territoire du Royaume, elles peuvent seulement être copiées. Dans ce cas, le juge d'instruction, par l'intermédiaire du ministère public, communique sans délai cette information au ministère de la Justice, qui en informe les autorités compétentes de l'état concerné, si celui-ci peut raisonnablement être déterminé.	Lorsqu'il s'avère que ces données ne se trouvent pas sur le territoire du Royaume, elles peuvent seulement être copiées. Dans ce cas, **le procureur du Roi** communique sans délai cette information au **Service public fédéral** Justice, qui en informe les autorités compétentes de l'état concerné, si celui-ci peut raisonnablement être déterminée.
§ 4. L'article 89bis est applicable à l'extension de la recherche dans un système informatique. ".	**En cas d'extrême urgence ou de flagrant délit, le procureur du Roi peut ordonner verbalement l'extension de la recherche visée à l'alinéa 1er. Cet ordre est confirmé par écrit dans les meilleurs délais, avec mention du flagrant délit ou des motifs de l'extrême urgence.** § 4 **Seul le juge d'instruction peut ordonner une recherche dans un système informatique ou une partie de celui-ci autre que les recherches visées aux paragraphes 2 et 3 :** - **si cette recherche est nécessaire pour la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche ; et** - **si d'autres mesures seraient disproportionnées, ou s'il existe**

	un risque que, sans cette recherche, des éléments de preuve soient perdus. **En cas d'extrême urgence, le juge d'instruction peut ordonner verbalement l'extension de la recherche visée à l'alinéa 1er. Cet ordre est confirmé par écrit dans les meilleurs délais, avec mention du flagrant délit ou des motifs de l'extrême urgence.** § 5. **En vue de permettre les mesures visée à cet article, le procureur du Roi ou le juge d'instruction peut également, sans le consentement du propriétaire ou de son ayant droit, ou de l'utilisateur, ordonner, à tout moment :** **- la suppression temporaire de toute protection des systèmes informatiques concernés, le cas échéant à l'aide de moyens techniques, de faux signaux, de fausses clés ou de fausses qualités ;** **- l'installation de dispositifs techniques dans les systèmes informatiques concernés en vue du décryptage et du décodage de données stockées, traitées ou transmises par ce système.** **Toutefois, seul le juge d'instruction peut ordonner cette suppression temporaire de protection ou cette installation de dispositifs techniques lorsque ceci est spécifiquement nécessaire pour l'application du paragraphe 3.**
(cf. §2)	§ 6. **Si** des données stockées **sont trouvées dans les systèmes informatiques concernés** qui sont utiles pour les mêmes finalités que celles prévues pour la saisie, mais que la saisie du support n'est néanmoins pas souhaitable, ces données, de même que les données nécessaires pour les comprendre, sont copiées sur des supports qui appartiennent à l'autorité. En cas d'urgence ou pour des raisons techniques, il peut être fait usage de supports qui sont disponibles pour des personnes autorisées à utiliser le système informatique.

(cf. §3, alinéa 1)	On utilise en outre les moyens techniques appropriés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité.
(cf. §4)	Lorsque la mesure prévue au § 2 n'est pas possible, pour des raisons techniques ou à cause du volume des données, **le procureur du Roi** utilise les moyens techniques appropriés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité.
(cf. §3, alinéa 2)	Si les données forment l'objet de l'infraction ou ont été produites par l'infraction et si elles sont contraires à l'ordre public ou aux bonnes mœurs ou constituent un danger pour l'intégrité des systèmes informatiques ou pour des données stockées, traitées ou transmises par le biais de tels systèmes, le procureur du Roi utilise tous les moyens techniques appropriés pour rendre ces données inaccessibles **ou, après en avoir pris copie, les retirer**.
(cf. §3, alinéa 3)	Il peut cependant, sauf dans le cas prévu à l'alinéa précédent, autoriser l'usage ultérieur de l'ensemble ou d'une partie de ces données, lorsque cela ne présente pas de danger pour l'exercice des poursuites. **En cas d'extrême urgence et s'il s'agit manifestement d'une infraction visée aux articles 137, § 3, 6°, 140bis ou 383bis, § 1er du Code pénal, le procureur du Roi peut ordonner verbalement que tous les moyens appropriés soient utilisés pour rendre inaccessibles les données qui forment l'objet de l'infraction ou ont été produites par l'infraction et qui sont contraires à l'ordre public ou aux bonnes mœurs. Cet ordre est confirmé par écrit dans les meilleurs délais, avec mention des motifs de l'extrême urgence.**
§ 5. Le procureur du Roi ou l'auditeur du	**§ 7. Sauf si son identité ou son adresse**

travail informe le responsable du système informatique de la recherche effectuée dans le système informatique et lui communique un résumé des données qui ont été copiées, rendues inaccessibles ou retirées.	**ne peuvent être raisonnablement retrouvées,** le procureur du Roi **ou le juge d'instruction** informe **dans les plus brefs délais** le responsable du système informatique de la recherche dans le système informatique **ou de son extension**. **Il** lui communique **le cas échéant** un résumé des données qui ont été copiées, rendues inaccessibles ou retirées.
§ 6. Le procureur du Roi ou l'auditeur du travail utilise les moyens techniques appropriés pour garantir l'intégrité et la confidentialité de ces données. Des moyens techniques appropriés sont utilisés pour leur conservation au greffe. La même règle s'applique, lorsque des données qui sont stockées, traitées ou transmises dans un système informatique sont saisies avec leur support, conformément aux articles précédents.	**§ 8**. Le procureur du Roi utilise les moyens techniques appropriés pour garantir l'intégrité et la confidentialité de ces données. Des moyens techniques appropriés sont utilisés pour leur conservation au greffe. La même règle s'applique, lorsque des données qui sont stockées, traitées ou transmises dans un système informatique sont saisies avec leur support, conformément aux articles précédents.
	Article 39ter (nouveau)
	§ 1er. Lors de la recherche de crimes et délits et sans préjudice des compétences visées aux articles 39bis, 46bis et 88bis du Code d'instruction criminelle et aux articles XII.17, XII.18, XII.19 et XII.20 du Code de droit économique, tout officier de police judiciaire peut, s'il existe des raisons de croire que des données stockées, traitées ou transmises par un système informatique au moyen d'un système informatique sont particulièrement susceptibles de perte ou de modification, ordonner, par une décision écrite motivée, à une ou plusieurs personnes physiques ou personnes morales de conserver les données qui sont en leur possession ou sous leur contrôle. **La décision écrite motivée mentionne :** - **les nom et qualité de l'officier de police judiciaire commis pour l'exécution de la mesure ;**

	- **l'infraction qui fait l'objet de la recherche ;** - **les données qui doivent être conservées ;** - **la durée de conservation des données, qui ne peut excéder nonante jours. Ce délai peut être prolongé par écrit.** **En cas d'urgence, la conservation peut être ordonnée verbalement. Elle doit être confirmée dans les plus brefs délais dans la forme prévue à l'alinéa précédent.** **§ 2. Les personnes physiques ou personnes morales visées au § 1er veillent à ce que l'intégrité des données soit garantie et à ce que les données soient conservées de manière sécurisée.** **§ 3. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.** **Toute personne qui refuse de coopérer, ou qui fait disparaître, détruit ou modifie les données conservées, sera punie d'un emprisonnement de six mois à un an ou d'une amende de 26 euros à 20.000 euros ou d'une de ces peines seulement.**
	Article 39quater (nouveau)
	§ 1er. Sans préjudice des possibilités de collaboration directe avec des opérateurs de services de communications électroniques et des fournisseurs de services de communications électroniques étrangers, le procureur du Roi peut, par l'intermédiaire du service de police désigné par le Roi, demander à une autorité compétente étrangère d'ordonner ou d'imposer d'une autre façon la conservation rapide de données stockées, traitées ou transmises par un système informatique qui se trouvent sur le territoire de cette autorité compétente et au sujet desquelles une autorité

	judiciaire belge compétente a l'intention de soumettre une demande d'entraide judiciaire. **La demande de conservation est formulée par écrit et mentionne :** - **les nom et qualité de l'autorité qui demande la conservation ;** - **l'infraction qui fait l'objet de la demande et un exposé succinct des faits qui y ont trait ;** - **les données à conserver et le lien avec l'infraction ;** - **toutes les informations disponibles concernant le dépositaire des données ou la localisation du système informatique ;** - **la nécessité de la conservation ;** - **le fait qu'une demande d'entraide judiciaire concernant les données conservées sera soumise ;** - **le cas échéant, le fait que les données qui doivent être conservées renvoient à un autre État que l'État de l'autorité étrangère compétente.** **§ 2. Lorsqu'une telle possibilité est prévue dans un instrument de droit international liant la Belgique et un autre Etat, une autorité compétente de cet Etat peut demander au service de police désigné par le Roi d'ordonner ou d'imposer d'une autre manière la conservation rapide de données stockées, traitées ou transmises par un système informatique qui se trouvent sur le territoire belge et au sujet desquelles cette autorité judiciaire étrangère a l'intention de soumettre une demande d'entraide judiciaire.** **La demande de conservation est formulée par écrit et mentionne :** - **les nom et qualité de l'autorité qui demande la conservation ;**

	- **l'infraction qui fait l'objet de la demande et un exposé succinct des faits qui y ont trait ;** - **les données à conserver et le lien avec l'infraction ;** - **toutes les informations disponibles concernant le dépositaire des données ou la localisation du système informatique ;** - **la nécessité de la conservation, et** - **le fait qu'une demande d'entraide judiciaire concernant les données conservées sera soumise ;** - **le cas échéant, le fait que les données qui doivent être conservées renvoient à un autre État que l'État de l'autorité étrangère compétente.** **Après réception de la demande visée à l'alinéa précédent, le service de police visé à l'alinéa 1er en informe le procureur du Roi ou le juge d'instruction compétent et prend toutes les mesures appropriées pour procéder sans délai à la conservation rapide des données définies conformément à l'article 39ter.** **Sans préjudice des instruments de droit international liant la Belgique en matière d'entraide judiciaire et tendant à promouvoir celle-ci, une demande de conservation peut être rejetée à tout moment par le procureur du Roi ou le juge d'instruction compétent :** - **si la demande concerne une infraction considérée par la Belgique comme une infraction politique ou un fait connexe à une infraction politique, ou** - **si l'exécution de la demande est de nature à porter atteinte à la souveraineté, à la sécurité, à l'ordre public ou à d'autres intérêts essentiels de la Belgique.** **Si le service de police visé à l'alinéa 1er estime que la conservation simple ne suffira pas à garantir la disponibilité**

	future des données, ou compromettra la confidentialité de l'enquête de l'autorité étrangère compétente ou nuira d'une autre façon à celle-ci, il en informe sans délai l'autorité étrangère compétente, qui décide alors s'il convient néanmoins d'exécuter la demande. **Une conservation effectuée en réponse à la demande visée à l'alinéa 1er est valable pour une période d'au moins 60 jours afin d'offrir à l'autorité étrangère compétente la possibilité de soumettre une demande d'entraide judiciaire. Après réception d'une telle demande, les données restent conservées dans l'attente d'une décision concernant la demande.** **Si les données qui sont stockées, traitées ou transmises par un système informatique renvoient à un autre État que l'État de l'autorité étrangère compétente requérante, le service de police visé à l'alinéa 1er en informe le procureur du Roi ou le juge d'instruction compétent. Celui-ci divulgue, dans les meilleurs délais, à l'autorité étrangère compétente une quantité de données d'identification ou d'appel suffisante pour retrouver qui est l'opérateur du réseau de communications électroniques ou le fournisseur du service de communications électroniques et par quelle voie la communication a été envoyée.**
Artikel 46bis	**Artikel 46bis**
§ 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	§ 1er. En recherchant les crimes et les délits, le procureur du Roi peut, par une décision motivée et écrite, procéder ou faire procéder sur la base de toutes données détenues par lui, ou au moyen d'un accès aux fichiers des clients **des acteurs visés à l'alinéa 2, 1er et 2e tirets**, à 1° l'identification de l'abonné ou de l'utilisateur habituel d'un **service visé à l'alinéa 2, deuxième tiret,** ou bien du

communication électronique utilise;	moyen de communication électronique utilisé ;
2° l'identification des services de communication électronique auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée.	2° l'identification des **services visés à l'alinéa 2, deuxième tiret,** auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée. **Si nécessaire, il peut pour ce faire requérir, directement ou par l'intermédiaire d'un service de police désigné par le Roi, la collaboration :** **- de l'opérateur d'un réseau de communications électroniques ;** **- de toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.**
La motivation reflète le caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête.	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.	En cas d'extrême urgence, **le procureur du Roi peut ordonner verbalement cette mesure. La décision est confirmée par écrit dans les plus brefs délais.** 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.
§ 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,	§ 2. **Les acteurs visés au § 1er, alinéa 2, 1er et 2e tirets**, requis de communiquer les données visées au § 1er **fournissent** au procureur du Roi ou à l'officier de police judiciaire les données qui ont été demandées **en temps réel ou, le cas échéant, au moment précisé dans la réquisition, selon les modalités fixées** par

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, 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. **Toute personne qui refuse de communiquer les données ou qui ne les communique pas en temps réel ou, le cas échéant, au moment précisé dans la réquisition** est punie d'une amende de vingt-six euros à dix mille euros.
Artikel 46quinquies	**Artikel 46quinquies**
§ 1er. Sans préjudice de l'article 89ter, le procureur du Roi peut, par une décision écrite et motivée, autoriser les services de police à pénétrer à tout moment dans un lieu privé, à l'insu du propriétaire ou de son ayant droit ou sans le consentement de ceux-ci, s'il existe des indices sérieux que les faits punissables constituent ou constitueraient une infraction visée à l'article 90ter, §§ 2 à 4, ou sont commis ou seraient commis dans le cadre d'une organisation criminelle visée à l'article 324bis du Code pénal, et si les autres moyens d'investigation ne semblent pas suffire à la manifestation de la vérité. Au sens du présent article, on entend par " lieu privé ", le lieu qui n'est manifestement pas : - un domicile; - une dépendance propre y enclose d'un domicile au sens des articles 479, 480 et 481 du Code pénal;	§ 1er. Sans préjudice de l'article 89ter, le procureur du Roi peut, par une décision écrite et motivée, autoriser les services de police à pénétrer à tout moment dans un lieu privé **et à ouvrir les objets fermés se trouvant dans ce lieu**, à l'insu du propriétaire ou de son ayant droit, ou sans le consentement de ceux-ci, s'il existe des indices sérieux que les faits punissables constituent ou constitueraient une infraction visée à l'article 90ter, §§ 2 à 4, ou sont commis ou seraient commis dans le cadre d'une organisation criminelle définie à l'article 324bis du Code pénal, et si les autres moyens d'investigation ne semblent pas suffire à la manifestation de la vérité. Au sens de cet article, on entend par "lieu privé" le lieu qui n'est manifestement pas : - un domicile ; - une dépendance propre y enclose d'un domicile au sens des articles 479, 480 et 481 du Code pénal ;

- un local utilisé à des fins professionnelles ou la résidence d'un avocat ou d'un médecin, visés à l'article 56bis, alinéa 3.	- un local utilisé à des fins professionnelles ou la résidence d'un avocat ou d'un médecin, visés à l'article 56bis, alinéa 3.
En cas d'urgence, la décision visée à l'alinéa 1er, peut être communiquée verbalement. En pareil cas, la décision doit être motivée et confirmée par écrit dans les plus brefs délais.	En cas d'urgence, la décision visée à l'alinéa 1er peut être communiquée verbalement. En pareil cas, la décision doit être motivée et confirmée par écrit dans les plus brefs délais.
Si la décision visée à l'alinéa 1er est prise dans le cadre de l'application de méthodes particulières de recherche visées aux articles 47ter à 47decies, la décision et tous les procès-verbaux y afférents sont joints au dossier répressif au plus tard après qu'il a été mis fin à la méthode particulière de recherche.	Si la décision visée à l'alinéa 1er est prise dans le cadre de l'application de méthodes particulières de recherche visées aux articles 47ter à 47decies, la décision et tous les procès-verbaux y afférents sont joints au dossier répressif au plus tard après qu'il a été mis fin à la méthode particulière de recherche.
§ 2. La pénétration dans le lieu privé visé au § 1er peut uniquement avoir lieu aux fins :	§ 2. La **pénétration du lieu privé visé au § 1er, et l'ouverture des objets fermés se trouvant sur ce lieu,** peuvent uniquement avoir lieu aux fins :
1° d'inspecter ce lieu et de s'assurer de la présence éventuelle de choses qui forment l'objet d'une infraction, qui ont servi ou qui sont destinées à en commettre une ou qui ont été produites par une infraction, des avantages patrimoniaux tirés directement de l'infraction, des biens et valeurs qui leur ont été substitués et des revenus de ces avantages investis;	1° d'inspecter ce lieu et de s'assurer de la présence éventuelle de choses qui forment l'objet d'une infraction, qui ont servi ou qui sont destinées à en commettre une ou qui ont été produites par une infraction, des avantages patrimoniaux tirés directement de l'infraction, des biens et valeurs qui leur ont été substitués et des revenus de ces avantages investis ;
2° de réunir les preuves de la présence des choses visées au 1°;	2° de réunir les preuves de la présence des choses visées au 1° ;
3° d'installer dans le cadre d'une observation un moyen technique visé à l'article 47sexies, § 1er, alinéa 3.	3° **de réparer ou de retirer** dans le cadre d'une observation un moyen technique visé à l'article 47sexies, § 1er, alinéa 3.
	4° de replacer les objets emportés conformément au § 5.
§ 3. Le procureur du Roi ne peut décider d'un contrôle visuel discret que pour des lieux où, sur la base d'indications précises, on suppose que se trouvent les choses visées au § 2, 1°, que des preuves peuvent en être collectées ou dont on suppose qu'ils sont utilisés par des personnes suspectes.	§ 3. Un contrôle visuel discret peut uniquement être décidé par le procureur du Roi pour des lieux où, sur la base d'indications précises, on suppose que se trouvent les choses visées au § 2, 1°, que des preuves peuvent en être collectées ou dont on suspecte qu'ils sont utilisés par des personnes suspectes.
§ 4. L'utilisation de moyens techniques aux fins visées au § 2, est assimilée à une	§ 4. L'utilisation de moyens techniques aux fins visées au § 2 est assimilée à une

pénétration dans un lieu privé vise au § 1er.	pénétration dans un lieu privé visé au § 1er. **§ 5. Si l'examen d'un objet visé au § 1er ne peut se faire sur place et si l'information ne peut être obtenue d'une autre manière, le service de police est autorisé à emporter cet objet pour une durée strictement limitée. L'objet en question est remis en place dans les plus brefs délais, à moins que cela n'entrave le bon déroulement de l'enquête.** **§ 6. Dans le cadre de la mesure visée au §1er, la pénétration dans un système informatique n'est possible qu'aux fins visées au § 2, 3°.** **§ 7. L'officier de police judiciaire qui dirige l'exécution de la mesure visé au §1er ou à l'article 89ter, §1er, rédige un procès-verbal du cours de la mesure. Lorsque des objets fermés sont ouverts ou qu'il est fait application du §5 durant l'exécution de la mesure, il en est fait mention dans le procès-verbal. Le procès-verbal est joint au dossier répressif au plus tard après qu'il a été mis fin à la mesure.**
	Article 46sexies (nouveau)
	§ 1er. Dans la recherche des crimes et délits, si les nécessités de l'enquête l'exigent et que les autres moyens d'investigation ne semblent pas suffire à la manifestation de la vérité, le procureur du Roi peut autoriser les services de police visés à l'alinéa 2 à entretenir, le cas échéant sous une identité fictive, des contacts avec une ou plusieurs personnes concernant lesquelles il existe des indices sérieux qu'elles commettent ou commettraient des infractions pouvant donner lieu à un emprisonnement correctionnel principal d'un an ou à une peine plus lourde. **Le Roi détermine les conditions, y compris pour ce qui concerne la formation, et les modalités de désignation des services de police habilités à exécuter la mesure visée au présent article.**

	Dans des circonstances exceptionnelles et moyennant l'autorisation expresse du procureur du Roi, le fonctionnaire de police visé à l'alinéa 1er peut, dans le cadre d'une opération déterminée, momentanément recourir à l'expertise d'une personne qui ne fait pas partie des services de police si cela s'avère strictement nécessaire à la réussite de sa mission. **Le présent article ne s'applique pas à l'interaction personnelle de fonctionnaires de police, dans l'exercice de leurs missions de police judiciaire, avec une ou plusieurs personnes sur Internet, qui n'a pour finalité directe qu'une vérification ciblée ou une arrestation, et ceci sans utiliser d'identité fictive crédible.** **§ 2. La mission visée au § 1er est ordonnée par le procureur du Roi par une autorisation écrite et motivée préalable. Cette autorisation est valable pour une période de trois mois, sous réserve de renouvellement.** **En cas d'urgence, l'autorisation peut être donnée verbalement. Elle doit être confirmée dans les plus brefs délais dans la forme prévue à l'alinéa précédent.** **§ 3. Sont exemptés de peine, les fonctionnaires de police qui, dans le cadre de leur mission et en vue de la réussite de celle-ci ou afin de garantir leur propre sécurité ou celle d'autres personnes, commettent des infractions strictement nécessaires, ce avec l'accord exprès du procureur du Roi.** **Ces infractions ne peuvent être plus graves que celles pour laquelle la mesure est utilisée et doivent nécessairement être proportionnelles à l'objectif visé.** **Les alinéas 1er et 2 sont également d'application aux personnes qui ont fourni directement une aide ou une assistance nécessaire à l'exécution de cette mission ainsi qu'aux personnes visées au § 1er, alinéa 3.**

	Sont exemptés de peine, les magistrats qui autorisent, dans le respect du présent code, un fonctionnaire de police et la personne visée à l'alinéa 3 à commettre des infractions dans le cadre de l'exécution de la mesure. **Les fonctionnaires de police communiquent, par écrit et préalablement à l'exécution de la mesure, au procureur du Roi les infractions qu'eux-mêmes ou les personnes visées à l'alinéa 3 ont l'intention de commettre.** **Si cette notification préalable n'a pas pu avoir lieu, les fonctionnaires de police informent sans délai le procureur du Roi des infractions qu'eux-mêmes ou les personnes visées à l'alinéa 3 ont commises et en donnent ensuite confirmation par écrit.** **Le procureur du Roi énonce dans une décision écrite séparée les infractions pouvant être commises par les services de police et les personnes visées à l'alinéa 3 dans le cadre de la mesure ordonnée par lui. Cette décision est conservée dans un dossier séparé et confidentiel. Il est le seul à avoir accès à ce dossier, sans préjudice du droit de consultation du juge d'instruction et de la chambre des mises en accusation visé respectivement à l'article 56bis et aux articles 235ter, § 3, et 235quater, § 3. Le contenu de ce dossier est couvert par le secret professionnel.** **§ 4. L'officier de police judiciaire chargé de l'enquête rédige le procès-verbal des différentes phases de l'exécution de cette mesure, y compris les contacts pertinents. Ces procès-verbaux sont joints au dossier au plus tard après la fin de la mesure.** **Les contacts visés au § 1er sont enregistrés avec les moyens techniques appropriés et joints au dossier ou déposés au greffe, sous forme numérique ou non, au plus tard après la fin de la mesure.** **§ 5. Le procureur du Roi est chargé de l'exécution des autorisations de la**

	mesure visée au § 1er, alinéa 1er, accordées par le juge d'instruction dans le cadre d'une instruction, conformément à l'article 56bis. **Le procureur du Roi énonce à ce moment dans une décision écrite séparée les infractions pouvant être commises par les services de police et les personnes visées au § 3, alinéa 3, dans le cadre de la mesure ordonnée par le juge d'instruction. Cette décision est conservée dans le dossier visé au § 3, alinéa 7.**
Article 47sexies	**Article 47sexies**
§ 1er. L'observation au sens du présent code est l'observation systématique, par un fonctionnaire de police, d'une ou de plusieurs personnes, de leur présence ou de leur comportement, ou de choses, de lieux ou d'événements déterminés. Une observation systématique au sens du présent code est une observation de plus de cinq jours consécutifs ou de plus de cinq jours non consécutifs répartis sur une période d'un mois, une observation dans le cadre de laquelle des moyens techniques sont utilisés, une observation revêtant un caractère international ou une observation exécutée par des unités spécialisées de la police fédérale. Un moyen technique au sens du présent code est une configuration de composants qui détecte des signaux, les transmet, active leur enregistrement et enregistre les signaux, à l'exception des moyens techniques utilisés en vue de l'exécution d'une mesure visée à l'article 90ter. Un appareil utilisé pour la prise de photographies n'est considéré comme moyen technique au sens du présent Code que dans le cas visé à l'article 56bis, alinéa 2. § 2. Le procureur du Roi peut, dans le cadre de l'information, autoriser une observation si les nécessités de l'enquête l'exigent et si les autres moyens	§ 1er. L'observation au sens du présent code est l'observation systématique, par un fonctionnaire de police, d'une ou de plusieurs personnes, de leur présence ou de leur comportement, ou de choses, de lieux ou d'événements déterminés. Une observation systématique au sens du présent code est une observation de plus de cinq jours consécutifs ou de plus de cinq jours non consécutifs répartis sur une période d'un mois, une observation dans le cadre de laquelle des moyens techniques sont utilisés, une observation revêtant un caractère international ou une observation exécutée par des unités spécialisées de la police fédérale. Un moyen technique au sens du présent code est une configuration de composants qui détecte des signaux, les transmet, active leur enregistrement et enregistre les signaux, à l'exception des moyens techniques utilisés en vue de l'exécution d'une mesure visée à l'article 90ter. Un appareil utilisé pour la prise de photographies n'est considéré comme moyen technique au sens du présent Code que dans le cas visé à l'article 56bis, alinéa 2. § 2. Le procureur du Roi peut, dans le cadre de l'information, autoriser une observation si les nécessités de l'enquête l'exigent et si les autres moyens d'investigation ne semblent

d'investigation ne semblent pas suffire à la manifestation de la vérité.	pas suffire à la manifestation de la vérité.
Une observation effectuée à l'aide de moyens techniques ne peut être autorisée que lorsqu'il existe des indices sérieux que les infractions sont de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde.	Une observation effectuée à l'aide de moyens techniques ne peut être autorisée que lorsqu'il existe des indices sérieux que les infractions sont de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde.
§ 3. L'autorisation de procéder à l'observation est écrite et contient les mentions suivantes:	§ 3. L'autorisation de procéder à l'observation est écrite et contient les mentions suivantes :
1° les indices sérieux de l'infraction qui justifient l'observation et, si l'observation s'inscrit dans le cadre de l'enquête proactive définie à l'article 28bis, § 2, les indices particuliers relatifs aux éléments décrits dans cette dernière disposition;	1° les indices sérieux de l'infraction qui justifient l'observation **ou,** si l'observation s'inscrit dans le cadre de l'enquête proactive définie à l'article 28bis, § 2, **la suspicion raisonnable que des faits punissables vont être commis ou ont été commis mais ne sont pas encore connus, et** les indices particuliers relatifs aux éléments décrits dans cette dernière disposition**, qui justifient l'observation** ;
2° les motifs pour lesquels l'observation est indispensable à la manifestation de la vérité;	2° les motifs pour lesquels l'observation est indispensable à la manifestation de la vérité ;
3° le nom ou, s'il n'est pas connu, une description aussi précise que possible de la ou des personnes observées, ainsi que des choses, des lieux ou des événements visés au § 1er;	3° le nom ou, s'il n'est pas connu, une description aussi précise que possible de la ou des personnes observées, ainsi que des choses, des lieux ou des événements visés au § 1er ;
4° la manière dont l'observation sera exécutée, y compris la permission d'utiliser des moyens techniques dans les cas prévus au § 2, alinéa 2, et à l'article 56bis, alinéa 2. Dans ce dernier cas, l'autorisation du juge d'instruction mentionne l'adresse ou une localisation aussi précise que possible de l'habitation qui fait l'objet de l'observation;	4° la manière dont l'observation sera exécutée, y compris la permission d'utiliser des moyens techniques dans les cas prévus au § 2, alinéa 2, et à l'article 56bis, alinéa 2. Dans ce dernier cas, l'autorisation du juge d'instruction mentionne l'adresse ou une localisation aussi précise que possible de l'habitation qui fait l'objet de l'observation ;
5° la période au cours de laquelle l'observation peut être exécutée et laquelle ne peut excéder un mois à compter de la date de l'autorisation;	5° la période au cours de laquelle l'observation peut être exécutée et laquelle ne peut excéder **trois mois** à compter de la date de l'autorisation ;
6° le nom et la qualité de l'officier de police judiciaire qui dirige l'exécution de l'observation.	6° le nom et la qualité de l'officier de police judiciaire qui dirige l'exécution de l'observation.
§ 4. Le procureur du Roi indique à ce moment dans une décision écrite séparée les infractions qui peuvent être commises	§ 4. Le procureur du Roi indique à ce moment dans une décision écrite séparée les infractions qui peuvent être commises

par les services de police et les personnes visées à l'article 47quinquies, § 2, troisième alinéa, dans le cadre de l'observation. Cette décision est conservée dans le dossier visé à l'article 47septies, § 1er, alinéa 2. § 5. En cas d'urgence, l'autorisation d'observation peut être accordée verbalement. Cette autorisation doit être confirmée dans les plus brefs délais dans la forme prévue à l'alinéa 1er. § 6. Le procureur du Roi peut à tout instant, de manière motivée, modifier, compléter ou prolonger son autorisation d'observation. Il peut à tout moment retirer son autorisation. Il vérifie si les conditions visées aux §§ 1er à 3, sont remplies chaque fois que son autorisation est modifiée, complétée ou prolongée et agit conformément au § 3, 1° à 6°. § 7. Le procureur du Roi est chargé de l'exécution des autorisations d'observation accordées par le juge d'instruction dans le cadre d'une instruction, conformément à l'article 56bis. Le procureur du Roi indique à ce moment dans une décision écrite séparée les infractions qui peuvent être commises par les services de police et les personnes visées à l'article 47quinquies, § 2, alinéa 3, dans le cadre de l'observation ordonnée par le juge d'instruction. Cette décision est conservée dans le dossier visé à l'article 47septies, § 1er, alinéa 2.	par les services de police et les personnes visées à l'article 47quinquies, § 2, alinéa 3, dans le cadre de l'observation. Cette décision est conservée dans le dossier visé à l'article 47septies, § 1er, alinéa 2. § 5. En cas d'urgence, l'autorisation d'observation peut être accordée verbalement. Elle doit être confirmée dans les plus brefs délais dans la forme prévue **au § 3**. § 6. Le procureur du Roi peut à tout instant, de manière motivée, modifier, compléter ou prolonger son autorisation d'observation. Il peut à tout moment retirer son autorisation. Il vérifie si les conditions visées aux §§ 1er à 3, sont remplies chaque fois que son autorisation est modifiée, complétée ou prolongée et agit conformément au § 3, 1° à 6°. § 7. Le procureur du Roi est chargé de l'exécution des autorisations d'observation accordées par le juge d'instruction dans le cadre d'une instruction, conformément à l'article 56bis. Le procureur du Roi indique à ce moment dans une décision écrite séparée les infractions qui peuvent être commises par les services de police et les personnes visées à l'article 47quinquies, § 2, alinéa 3, dans le cadre de l'observation ordonnée par le juge d'instruction. Cette décision est conservée dans le dossier visé à l'article 47septies, § 1er, alinéa 2.
Article 47octies	**Article 47octies**
§ 1er. L'infiltration au sens du présent code est le fait, pour un fonctionnaire de police, appelé infiltrant, d'entretenir, sous une identité fictive, des relations durables avec une ou plusieurs personnes concernant lesquelles il existe des indices sérieux qu'elles commettent ou commettraient des infractions dans le cadre d'une organisation criminelle visée à l'article 324bis du Code pénal ou des crimes ou des délits visés à l'article 90ter, §§ 2 à 4. L'infiltrant peut, dans des circonstances	§ 1er. L'infiltration au sens du présent code est le fait, pour un fonctionnaire de police, appelé infiltrant, d'entretenir, sous une identité fictive, des relations durables avec une ou plusieurs personnes concernant lesquelles il existe des indices sérieux qu'elles commettent ou commettraient des infractions dans le cadre d'une organisation criminelle visée à l'article 324bis du Code pénal ou des crimes ou des délits visés à l'article 90ter, §§ 2 à 4. L'infiltrant peut, dans des circonstances

exceptionnelles et moyennant l'autorisation expresse du magistrat compétent, recourir brièvement, dans le cadre d'une opération spécifique, à l'expertise d'une personne externe aux services de police si cela s'avère absolument indispensable à la réussite de sa mission.	exceptionnelles et moyennant l'autorisation expresse du magistrat compétent, recourir brièvement, dans le cadre d'une opération spécifique, à l'expertise d'une personne externe aux services de police si cela s'avère absolument indispensable à la réussite de sa mission.
§ 2. Le procureur du Roi peut, dans le cadre de l'information, autoriser une infiltration si les nécessités de l'enquête l'exigent et si les autres moyens d'investigation ne semblent pas suffire à la manifestation de la vérité.	§ 2. Le procureur du Roi peut, dans le cadre de l'information, autoriser une infiltration si les nécessités de l'enquête l'exigent et si les autres moyens d'investigation ne semblent pas suffire à la manifestation de la vérité.
Il peut autoriser le service de police à appliquer certaines techniques d'enquête policières dans le cadre légal d'une infiltration et compte tenu de la finalité de celle-ci. Le Roi détermine par arrêté délibéré en Conseil des Ministres ces techniques d'enquête policières, sur proposition du ministre de la Justice et sur avis du Collège des procureurs généraux. Ces techniques d'enquête policières ne peuvent être mises en oeuvre que par des membres de la direction des unités spéciales de la police fédérale et, le cas échéant, moyennant l'accord préalable supplémentaire du procureur fédéral, en collaboration avec des fonctionnaires compétents étrangers spécifiquement formés à cet effet.	Il peut autoriser le service de police à appliquer certaines techniques d'enquête policières dans le cadre légal d'une infiltration et compte tenu de la finalité de celle-ci. Le Roi détermine par arrêté délibéré en Conseil des ministres ces techniques d'enquête policières, sur proposition du ministre de la Justice et sur avis du Collège des procureurs généraux. Ces techniques d'enquête policières ne peuvent être mises en œuvre que par des membres de la direction des unités spéciales de la police fédérale et, le cas échéant, moyennant l'accord préalable supplémentaire du procureur fédéral, en collaboration avec des fonctionnaires compétents étrangers spécifiquement formés à cet effet.
Si c'est justifié, le procureur du Roi accorde l'autorisation de prendre les mesures nécessaires en vue de garantir la sécurité, ainsi que l'intégrité physique, psychique et morale de l'infiltrant. Cette autorisation est conservée dans le dossier confidentiel visé à l'article 47novies, § 1er, alinéa 2.	Si c'est justifié, le procureur du Roi accorde l'autorisation de prendre les mesures nécessaires en vue de garantir la sécurité, ainsi que l'intégrité physique, psychique et morale de l'infiltrant. Cette autorisation est conservée dans le dossier confidentiel visé à l'article 47novies, § 1er, alinéa 2.
§ 3. L'autorisation d'infiltration est écrite et contient les mentions suivantes :	§ 3. L'autorisation d'infiltration est écrite et contient les mentions suivantes :
1° les indices sérieux de l'infraction qui justifient l'infiltration;	1° les indices sérieux de l'infraction qui justifient l'infiltration **ou, si l'infiltration s'inscrit dans le cadre de l'enquête proactive définie à l'article 28bis, § 2, la suspicion raisonnable que des faits punissables vont être commis ou ont été commis mais ne sont pas encore connus, et les indices particuliers relatifs aux éléments décrits dans cette dernière disposition, qui justifient l'infiltration ;**
2° les motifs pour lesquels l'infiltration est	2° les motifs pour lesquels l'infiltration est

indispensable à la manifestation de la vérité;	indispensable à la manifestation de la vérité ;
3° s'il est connu, le nom ou, sinon, une description aussi précise que possible de la ou des personnes visées au § 1er;	3° s'il est connu, le nom ou, sinon, une description aussi précise que possible de la ou des personnes visées au § 1er ;
4° la manière dont l'infiltration sera exécutée, y compris l'autorisation de recourir brièvement à l'expertise d'un civil conformément au § 1er, alinéa 2, ainsi que l'autorisation d'appliquer des techniques d'enquête policières, conformément au § 2, alinéa 2;	4° la manière dont l'infiltration sera exécutée, y compris l'autorisation de recourir brièvement à l'expertise d'un civil conformément au § 1er, alinéa 2, ainsi que l'autorisation d'appliquer des techniques d'enquête policières, conformément au § 2, alinéa 2 ;
5° la période au cours de laquelle l'infiltration peut être exécutée et laquelle ne peut excéder trois mois à compter de la date de l'autorisation;	5° la période au cours de laquelle l'infiltration peut être exécutée et laquelle ne peut excéder trois mois à compter de la date de l'autorisation ;
6° le nom et la qualité de l'officier de police judiciaire qui dirige l'exécution de l'infiltration.	6° le nom et la qualité de l'officier de police judiciaire qui dirige l'exécution de l'infiltration.
§ 4. Le procureur du Roi indique à ce moment dans une décision écrite séparée les infractions qui peuvent être commises par les services de police et les personnes visées à l'article 47quinquies, § 2, alinéa 3, dans le cadre de l'infiltration. Cette décision est conservée dans le dossier visé à l'article 47novies, § 1er, alinéa 2.	§ 4. Le procureur du Roi indique à ce moment dans une décision écrite séparée les infractions qui peuvent être commises par les services de police et les personnes visées à l'article 47quinquies, § 2, alinéa 3, dans le cadre de l'infiltration. Cette décision est conservée dans le dossier visé à l'article 47novies, § 1er, alinéa 2.
§ 5. En cas d'urgence, l'autorisation d'infiltration peut être accordée verbalement. Cette autorisation doit être confirmée dans les plus brefs délais dans la forme prévue à l'alinéa 1er.	§ 5. En cas d'urgence, l'autorisation d'infiltration peut être accordée verbalement. Elle doit être confirmée dans les plus brefs délais dans la forme prévue **au § 3**.
§ 6. Le procureur du Roi peut à tout instant, de manière motivée, modifier, compléter ou prolonger son autorisation d'infiltration. Il peut à tout moment retirer son autorisation. Il vérifie si les conditions visées aux §§ 1er à 3 sont remplies chaque fois que son autorisation est modifiée, complétée ou prolongée et agit conformément au § 3, 1° à 6°.	§ 6. Le procureur du Roi peut à tout instant, de manière motivée, modifier, compléter ou prolonger son autorisation d'infiltration. Il peut à tout moment retirer son autorisation. Il vérifie si les conditions visées aux §§ 1er à 3, sont remplies chaque fois que son autorisation est modifiée, complétée ou prolongée et agit conformément au § 3, 1° à 6°.
§ 7. Le procureur du Roi est chargé de l'exécution des autorisations d'infiltration accordées par le juge d'instruction dans le cadre d'une instruction, conformément à l'article 56bis.	§ 7. Le procureur du Roi est chargé de l'exécution des autorisations d'infiltration accordées par le juge d'instruction dans le cadre d'une instruction, conformément à l'article 56bis.
Le procureur du Roi indique à ce moment dans une décision écrite séparée les	Le procureur du Roi indique à ce moment dans une décision écrite séparée les

infractions qui peuvent être commises par les services de police et les personnes visées à l'article 47quinquies, § 2, alinéa 3, dans le cadre de l'infiltration ordonnée par le juge d'instruction. Cette décision est conservée dans le dossier vise à l'article 47novies, § 1er, alinéa 2.	infractions qui peuvent être commises par les services de police et les personnes visées à l'article 47quinquies, § 2, alinéa 3, dans le cadre de l'infiltration ordonnée par le juge d'instruction. Cette décision est conservée dans le dossier visé à l'article 47novies, § 1er, alinéa 2.
Article 47undecies	**Article 47undecies**
Au moins tous les trois mois, le procureur du Roi transmet au procureur général tous les dossiers dans lesquels il a fait application de méthodes particulières de recherche d'observation et d'infiltration, et dans lesquels il a pris la décision de ne pas engager de poursuites, afin de lui permettre d'exercer un contrôle sur la légalité des méthodes utilisées. Le procureur général fait rapport de ce contrôle. Le rapport est communiqué au collège des procureurs généraux, qui intègre l'évaluation globale et les données statistiques relatives à ces rapports dans son rapport annuel visé à l'article 143bis, § 7, du Code judiciaire. Le procureur fédéral publie dans son rapport annuel, visé à l'article 346, § 2, 2°, du même Code, l'évaluation globale et les données statistiques relatives aux dossiers dans lesquels il a fait application de méthodes particulières de recherche d'observation et d'infiltration, et dans lesquels il a pris la décision de ne pas engager de poursuites. Le collège des procureurs généraux exerce un contrôle sur tous les dossiers dans lesquels le recours aux indicateurs conformément à l'article 47decies, § 7, a été mis en oeuvre. A cette fin, un rapport circonstancié est transmis au président du collège des procureurs généraux par le procureur du Roi par la voie du procureur général territorialement compétent, ou directement par le procureur fédéral. Ce rapport est transmis dès qu'il est mis fin à l'application de cette méthode particulière de recherche. Le collège des procureurs généraux fait rapport de ce contrôle et intègre l'évaluation globale et les données statistiques relatives à ce sujet dans son rapport annuel visé à l'article 143bis, § 7, du	Au moins tous les trois mois, le procureur du Roi transmet au procureur général tous les dossiers dans lesquels il a fait application de méthodes particulières de recherche d'observation et d'infiltration, et dans lesquels il a pris la décision de ne pas engager de poursuites, afin de lui permettre d'exercer un contrôle sur la légalité des méthodes utilisées. Le procureur général fait rapport de ce contrôle. Le rapport est communiqué au Collège des procureurs généraux, qui intègre l'évaluation globale et les données statistiques relatives à ces rapports dans son rapport annuel visé à l'article 143bis, § 7, du Code judiciaire. Le procureur fédéral publie dans son rapport annuel, visé à l'article 346, § 2, 2°, du même Code, l'évaluation globale et les données statistiques relatives aux dossiers dans lesquels il a fait application de méthodes particulières de recherche d'observation et d'infiltration, et dans lesquels il a pris la décision de ne pas engager de poursuites.

Code judiciaire.	
Article 56bis	**Article 56bis**
Par dérogation à l'article 56, § 1er, alinéa 3, les autorisations du juge d'instruction par lesquelles il ordonne des méthodes particulières de recherche sont exécutées par le procureur du Roi. Il est procédé conformément aux articles 47ter à 47novies.	Par dérogation à l'article 56, § 1er, alinéa 3, les autorisations du juge d'instruction par lesquelles il ordonne des méthodes particulières de recherche **ou une mesure visée à l'article 46sexies** sont exécutées par le procureur du Roi. Il est procédé conformément aux articles 47ter à 47novies **et 46sexies respectivement**.
Seul le juge d'instruction peut en outre autoriser une observation, visée à l'article 47sexies, effectuée à l'aide de moyens techniques afin d'avoir une vue dans un domicile, ou dans une dépendance propre y enclose de ce domicile au sens des articles 479, 480 et 481 du Code pénal, ou dans un local utilisé à des fins professionnelles ou comme résidence par un avocat ou un médecin, visé à l'alinéa 3, lorsqu'il existe des indices sérieux que les faits punissables constituent ou constitueraient une infraction visée à l'article 90ter, §§ 2 à 4, ou sont ou seraient commis dans le cadre d'une organisation criminelle visée à l'article 324bis du Code pénal.	Seul le juge d'instruction peut en outre autoriser une observation, visée à l'article 47sexies, effectuée à l'aide de moyens techniques afin d'avoir une vue dans un domicile, ou dans une dépendance propre y enclose de ce domicile au sens des articles 479, 480 et 481 du Code pénal, ou dans un local utilisé à des fins professionnelles ou comme résidence par un avocat ou un médecin, visé à l'alinéa 3, lorsqu'il existe des indices sérieux que les faits punissables constituent ou constitueraient une infraction visée à l'article 90ter, §§ 2 à 4, ou sont ou seraient commis dans le cadre d'une organisation criminelle visée à l'article 324bis du Code pénal.
Une observation, comme prévue à l'alinéa précédent, une infiltration comme prévue à l'article 47octies, ou un contrôle visuel discret comme prévu à l'article 89ter qui porte sur les locaux utilisés à des fins professionnelles ou la résidence d'un avocat ou d'un médecin, peut uniquement être autorisée par le juge d'instruction si l'avocat ou le médecin est lui-même soupçonné d'avoir commis une des infractions visées à l'article 90ter, §§ 2 à 4, ou une infraction dans le cadre d'une organisation criminelle visée à l'article 324bis du Code pénal, ou si des faits précis laissent présumer que des tiers soupçonnés d'avoir commis une de ces infractions utilisent ses locaux ou sa résidence.	Une observation, comme prévue à l'alinéa précédent, une infiltration comme prévue à l'article 47octies, ou un contrôle visuel discret comme prévu à l'article 89ter qui porte sur les locaux utilisés à des fins professionnelles ou la résidence d'un avocat ou d'un médecin, peut uniquement être autorisé par le juge d'instruction si l'avocat ou le médecin est lui-même soupçonné d'avoir commis une des infractions visées à l'article 90ter, §§ 2 à 4, ou une infraction dans le cadre d'une organisation criminelle visée à l'article 324bis du Code pénal, ou si des faits précis laissent présumer que des tiers soupçonnés d'avoir commis une de ces infractions utilisent ses locaux ou sa résidence.
Ces mesures ne peuvent être exécutées sans que le bâtonnier ou le représentant de l'ordre provincial des médecins en soit averti.	Ces mesures ne peuvent être exécutées sans que le bâtonnier ou le représentant de l'ordre provincial des médecins en soit averti. **Ces personnes sont tenues au secret. Toute violation du secret est punie**

	conformément à l'article 458 du Code pénal.
Dans son instruction, le juge d'instruction a le droit de consulter à tout moment le dossier confidentiel concernant l'exécution des méthodes particulières de recherche, sans pouvoir faire mention de son contenu dans le cadre de son instruction. Il peut toujours, de manière motivée, modifier, compléter ou prolonger l'autorisation. Il peut à tout instant retirer l'autorisation. Il vérifie si les conditions relatives à la méthode particulière de recherche sont remplies chaque fois que l'autorisation est modifiée, complétée ou prolongée.	Dans son instruction, le juge d'instruction a le droit de consulter à tout moment le dossier confidentiel concernant l'exécution des méthodes particulières de recherche, sans pouvoir faire mention de son contenu dans le cadre de son instruction. Il peut toujours, de manière motivée, modifier, compléter ou prolonger l'autorisation. Il peut à tout moment retirer l'autorisation. Il vérifie si les conditions relatives à la méthode particulière de recherche sont remplies chaque fois que l'autorisation est modifiée, complétée ou prolongée.
Le juge d'instruction confirme par ordonnance écrite l'existence de l'autorisation de la méthode particulière de recherche qu'il a accordée.	Le juge d'instruction confirme par ordonnance écrite l'existence de l'autorisation de la méthode particulière de recherche qu'il a accordée.
Les procès-verbaux rédigés, ainsi que l'ordonnance visée à l'alinéa précédent, sont joints au dossier répressif au plus tard après qu'il est mis fin à la méthode particulière de recherche.	Les procès-verbaux rédigés, ainsi que l'ordonnance visée à l'alinéa précédent, sont joints au dossier répressif au plus tard après qu'il est mis fin à la méthode particulière de recherche.
Article 88bis	**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 :	§ 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 :
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 ;	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° à la localisation de l'origine ou de la destination de communications électroniques. **Si nécessaire, il peut pour ce faire requérir, directement ou par l'intermédiaire d'un service de police désigné par le Roi, la collaboration :** **- de l'opérateur d'un réseau de communications électroniques ; et** **- de toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.**
Dans les cas visés à l'alinéa 1er, pour chaque 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.	Dans les cas visés à l'alinéa 1er, pour chaque 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, son caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête, dans une ordonnance motivée.	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 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.	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.	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.	S'il s'agit toutefois de l'infraction visée à l'article 347bis**, 434** 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.	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.	S'il s'agit toutefois de l'infraction visée à l'article 347bis**, 434** 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.	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 4 **et 5**.
§ 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 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	§ 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 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 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.	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.
§ 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.	§ 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.	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. **Ces personnes sont tenues au secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.**
§ 4. 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.	§ 4. **Les acteurs visés au § 1er, alinéa 2, communiquent** les informations demandées **en temps réel ou, le cas échéant, au moment précisé dans la réquisition, selon les modalités fixées** 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, 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	Toute personne qui refuse de prêter son concours technique aux réquisitions visées au présent article, concours dont les modalités sont fixées 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 à dix mille francs.	ministre compétent pour les Télécommunications, **ou ne le prête pas en temps réel ou, le cas échéant, au moment précisé dans la réquisition,** est punie d'une amende de vingt-six francs à dix mille francs.
Article 88ter	**Article 88ter**
§ 1er. Lorsque le juge d'instruction ordonne une recherche dans un système informatique ou une partie de celui-ci, cette recherche peut être étendue vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée : - si cette extension est nécessaire pour la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche, et - si d'autres mesures seraient disproportionnées, ou s'il existe un risque que, sans cette extension, des éléments de preuve soient perdus. § 2. L'extension de la recherche dans un système informatique ne peut pas excéder les systèmes informatiques ou les parties de tels systèmes auxquels les personnes autorisées à utiliser le système informatique qui fait l'objet de la mesure ont spécifiquement accès. § 3. En ce qui concerne les données recueillies par l'extension de la recherche dans un système informatique, qui sont utiles pour les mêmes finalités que celles prévues pour la saisie, les règles prévues à l'article 39bis s'appliquent. Le juge d'instruction informe le responsable du système informatique, sauf si son identité ou son adresse ne peuvent être raisonnablement retrouvées. Lorsqu'il s'avère que ces données ne se trouvent pas sur le territoire du Royaume, elles peuvent seulement être copiées. Dans ce cas, le juge d'instruction, par l'intermédiaire du ministère public, communique sans délai cette information au ministère de la Justice, qui en informe les autorités compétentes de l'état concerné, si celui-ci peut raisonnablement être déterminé.	Abrogé

§ 4. L'article 89bis est applicable à l'extension de la recherche dans un système informatique.	
Article 88quater	**Article 88quater**
§ 1er. Le juge d'instruction ou un officier de police judiciaire auxiliaire du procureur du Roi et de l'auditeur du travail délégué par lui, peut ordonner aux personnes dont il présume qu'elles ont une connaissance particulière du système informatique qui fait l'objet de la recherche ou des services qui permettent de protéger ou de crypter des données qui sont stockées, traitées ou transmises par un système informatique, de fournir des informations sur le fonctionnement de ce système et sur la manière d'y accéder ou d'accéder aux données qui sont stockées, traitées ou transmises par un tel système, dans une forme compréhensible. Le juge d'instruction mentionne les circonstances propres à l'affaire justifiant la mesure dans une ordonnance motivée qu'il transmet au procureur du Roi ou à l'auditeur du travail.	§ 1er. Le juge d'instruction ou un officier de police judiciaire auxiliaire du procureur du Roi et de l'auditeur du travail délégué par lui, peut ordonner **à quiconque** dont il présume qu'elles ont une connaissance particulière du système informatique qui fait l'objet de la recherche **ou de son extension visée à l'article 39bis** ou des services qui permettent de protéger ou de crypter des données qui sont stockées, traitées ou transmises par un système informatique, de fournir des informations sur le fonctionnement de ce système et sur la manière d'y accéder ou d'accéder aux données qui sont stockées, traitées ou transmises par un tel système, dans une forme compréhensible. Le juge d'instruction mentionne les circonstances propres à l'affaire justifiant la mesure dans une ordonnance motivée qu'il transmet au procureur du Roi ou à l'auditeur du travail.
§ 2. Le juge d'instruction ou un officier de police judiciaire auxiliaire du procureur du Roi et de l'auditeur du travail délégué par lui, peut ordonner à toute personne appropriée de mettre en fonctionnement elle-même le système informatique ou, selon le cas, de rechercher, rendre accessibles, copier, rendre inaccessibles ou retirer les données pertinentes qui sont stockées, traitées ou transmises par ce système, dans la forme qu'il aura demandée. Ces personnes sont tenues d'y donner suite, dans la mesure de leurs moyens. L'ordonnance vises à l'alinéa 1er, ne peut être prise à l'égard de l'inculpé et à l'égard des personnes visées à l'article 156.	§ 2. Le juge d'instruction ou un officier de police judiciaire auxiliaire du procureur du Roi et de l'auditeur du travail délégué par lui peut ordonner à toute personne appropriée de mettre en fonctionnement elle-même le système informatique ou, selon le cas, de rechercher, rendre accessibles, copier, rendre inaccessibles ou retirer les données pertinentes qui sont stockées, traitées ou transmises par ce système, dans la forme qu'il aura demandée. Ces personnes sont tenues d'y donner suite, dans la mesure de leurs moyens. L'ordonnance visée à l'alinéa 1er, ne peut être prise à l'égard de l'inculpé et à l'égard des personnes visées à l'article 156.
§ 3. Celui qui refuse de fournir la collaboration ordonnée aux §§ 1er et 2 ou qui fait obstacle à la recherche dans le système informatique, est puni d'un emprisonnement de six mois à un an et d'une amende de vingt-six francs à vingt	§ 3. Celui qui refuse de fournir la collaboration ordonnée aux §§ 1er et 2 ou qui fait obstacle à la recherche **ou à son extension** dans le système informatique, est puni d'un emprisonnement de six mois à **trois ans** et d'une amende de vingt-six

mille francs ou d'une de ces peines seulement.	francs à vingt mille francs ou d'une de ces peines seulement. **Si la collaboration visée à l'alinéa 1er peut empêcher la commission d'un crime ou d'un délit ou peut en limiter les effets et que cette collaboration n'est pas fournie, les peines sont un emprisonnement de un à cinq ans et une amende de cinq cents euros à cinquante mille euros.**
§ 4. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.	§ 4. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.
§ 5. L'Etat est civilement responsable pour le dommage causé de façon non intentionnelle par les personnes requises à un système informatique ou aux données qui sont stockées, traitées ou transmises par un tel système.	§ 5. L'État est civilement responsable pour le dommage causé de façon non intentionnelle par les personnes requises à un système informatique ou aux données qui sont stockées, traitées ou transmises par un tel système.
Article 89ter	**Article 89ter**
Dans le cadre de l'exécution de la mesure prévue à l'article 46quinquies, et aux conditions qu'il énonce, seul le juge d'instruction peut autoriser les services de police à pénétrer à tout moment dans un lieu privé autre que celui visé à l'article 46quinquies, § 1er, à l'insu du propriétaire ou de son ayant droit, ou de l'occupant, ou sans le consentement de ceux-ci.	Dans le cadre de l'exécution de la mesure prévue à l'article 46quinquies, et aux conditions **ainsi qu'aux fins** qu'il énonce, seul le juge d'instruction peut autoriser le service de police **désigné par le Roi** à : - pénétrer à tout moment dans un lieu privé autre que celui visé à l'article 46quinquies, § 1er, **en ce compris ouvrir les objets fermés se trouvant dans ce lieu,** à l'insu du propriétaire ou de son ayant droit, ou de l'occupant, ou sans le consentement de ceux-ci **;** - **s'introduire dans un système informatique et l'explorer, à l'insu du propriétaire, du détenteur ou de l'utilisateur ou sans leur consentement, sans préjudice de la possibilité pour le procureur du Roi d'autoriser l'introduction dans un système informatique dans les limites visées à l'article 46quinquies, § 6.**
Si l'autorisation visée à l'alinéa 1er est accordée dans le cadre de l'application de méthodes particulières de recherche conformément aux articles 47ter à 47decies	Si l'autorisation visée à l'alinéa 1er est accordée dans le cadre de l'application de méthodes particulières de recherche conformément aux articles 47ter à 47decies

ou à l'article 56bis, l'autorisation et tous les procès-verbaux y afférents sont joints au dossier répressif au plus tard après qu'il a été mis fin à la méthode particulière de recherche. Il communique une copie de son ordonnance au procureur du Roi.	ou à l'article 56bis, l'autorisation et tous les procès-verbaux y afférents sont joints au dossier répressif au plus tard après qu'il a été mis fin à la méthode particulière de recherche. Il communique une copie de son ordonnance au procureur du Roi.
§6. DES ECOUTES, DE LA PRISE DE CONNAISSANCE ET DE L'ENREGISTREMENT DE COMMUNICATIONS ET DE TELECOMMUNICATIONS PRIVEES.	**§ 6. INTERCEPTER, PRENDRE CONNAISSANCE, EXPLORER ET ENREGISTRER DES COMMUNICATIONS NON ACCESSIBLES AU PUBLIC OU DES DONNEES D'UN SYSTEME INFORMATIQUE OU D'UNE PARTIE DE CELUI-CI.**
Article 90ter	**Article 90ter**
§ 1. Lorsque les nécessités de l'instruction l'exigent, le juge d'instruction peut, à titre exceptionnel, écouter, prendre connaissance et enregistrer, pendant leur transmission, des communications ou des télécommunications privées, s'il existe des indices sérieux que le fait dont il est saisi constitue une infraction visée par l'une des dispositions énumérées au § 2, et si les autres moyens d'investigation ne suffisent pas à la manifestation de la vérité. En vue de permettre l'écoute, la prise de connaissance ou l'enregistrement direct de communications ou télécommunications privées à l'aide de moyens techniques, le juge d'instruction peut également à l'insu ou sans le consentement de l'occupant, du propriétaire ou de ses ayants droit, ordonner la pénétration , à tout moment, dans un domicile ou dans un lieu privé.	§ 1er. **Sans préjudice de l'application des articles 39bis, 87, 88, 89bis et 90, le juge d'instruction peut, dans un but secret, intercepter, prendre connaissance, explorer et enregistrer, à l'aide de moyens techniques, des communications non accessibles au public ou des données d'un système informatique ou d'une partie de celui-ci, ou étendre une recherche dans un système informatique ou une partie de celui-ci.** **Cette mesure ne peut être ordonnée que dans des cas exceptionnels, lorsque les nécessités de l'instruction l'exigent, s'il existe des indices sérieux que cela concerne une infraction visée par l'une des dispositions énumérées au § 2, et si les autres moyens d'investigation ne suffisent pas à la manifestation de la vérité.** En vue de permettre **cette mesure**, le juge d'instruction peut également, à l'insu ou sans le consentement de l'occupant, du propriétaire ou de son ayant droit, **ou de l'utilisateur**, ordonner, à tout moment : **- la pénétration dans un domicile, un lieu privé ou un système informatique ;** **- la suppression temporaire de toute protection des systèmes informatiques concernés, le cas échéant à l'aide de moyens techniques, de faux signaux, de fausses clés ou de fausses qualités ;**

	- l'installation de dispositifs techniques dans les systèmes informatiques concernés en vue du décryptage et du décodage de données stockées, traitées ou transmises par ce système.
La mesure de surveillance ne peut être ordonnée qu'à l'égard soit de personnes soupçonnées, sur la base d'indices précis, d'avoir commis l'infraction, soit à l'égard des moyens de communication ou de télécommunication régulièrement utilisés par un suspect, soit à l'égard des lieux présumés fréquentés par celui-ci. Elle peut l'être également à l'égard de personnes présumées, sur la base de faits précis, être en communication régulière avec un suspect.	**La mesure visée dans ce paragraphe peut uniquement être ordonnée pour rechercher les données qui peuvent servir à la manifestation de la vérité. Elle** ne peut être ordonnée qu'à l'égard soit de personnes soupçonnées, sur la base d'indices précis, d'avoir commis l'infraction, soit à l'égard des moyens de communication ou systèmes informatiques régulièrement utilisés par un suspect, soit à l'égard des lieux présumés fréquentés par celui-ci. Elle peut également **être ordonnée** à l'égard de personnes présumées, sur la base de faits précis, être en communication régulière avec un suspect.
§ 2. Les infractions pouvant justifier une mesure de surveillance sont celles qui sont visées :	§ 2. Les infractions pouvant justifier **la mesure visée au § 1er** sont celles qui sont visées :
1° aux articles 101 à 110 du Code pénal;	1° aux articles 101 à 110 du Code pénal ;
1°bis. Les articles 136bis, 136ter, 136quater, 136sexies et 136septies du même Code et l'article 41 de la loi du 29 mars 2004 concernant la coopération avec la Cour pénale internationale et les tribunaux pénaux internationaux;	**2° aux** articles 136bis, 136ter, 136quater, 136sexies et 136septies du même Code et **à** l'article 41 de la loi du 29 mars 2004 concernant la coopération avec la Cour pénale internationale et les tribunaux pénaux internationaux ;
1°ter au livre II, titre Ierter, du même Code;	**3°** au livre II, titre Iter, du même Code ;
	4° à l'article 147 du même Code ;
	5° aux articles 160, 161, 162, 163, 168, 171, 173 et 176 du même Code ;
	6° aux articles 180 et 186 du même Code ;
1°quater à l'article 210bis du même Code;	**7°** à l'article 210bis du même Code ;
1°quinquies aux articles 246, 247, 248, 249, 250 et 251 du même Code;	**8°** aux articles 246, 247, 248, 249 et 250 du même Code ;
1°sexies à l'article 259bis du même Code;	**9°** à l'article 259bis du même Code ;
1°septies à l'article 314bis du même Code;	**10°** à l'article 314bis du même Code ;

1°octies aux articles 324bis et 324ter du même Code.	**11°** aux articles 324bis et 324ter du même Code ;
2° aux articles 327, 328, 329 ou 330 du même Code, pour autant qu'une plainte ait été déposée;	**12°** aux articles 327, 328, 329 ou 330 du même Code, pour autant qu'une plainte ait été déposée ;
3° à l'article 331bis du même Code;	**13°** à l'article 331bis du même Code ;
4° a l'article 347bis du même Code;	**14°** à l'article 347bis du même Code ;
4°bis	**15° aux articles 372 à 377bis du même Code** ; **16° à l'article 377quater du même Code** ;
5° Aux articles 379 et 380 du même Code.	**17°** aux articles 379, 380 **et 383bis, §§ 1er et 3,** du même Code ;
6° à l'article 393 du même Code;	**18°** à l'article 393 du même Code ;
7° aux articles 394 ou 397 du même Code;	**19°** aux articles 394 ou 397 du même Code ;
7°bis. Aux articles 428 et 429 du même Code;	**20°** aux articles 428 et 429 du même Code ; **21° à l'article 433bis/1 du même Code** ;
7°ter. aux articles 433sexies, 433septies et 433octies du même Code;	**22°** aux articles **433quinquies à** 433octies du même Code ; **23° à l'article 434 du même Code** ;
8° aux articles 468, 470, 471 ou 472 du même Code;	**24°** aux articles 468, 470, 471 ou 472 du même Code ;
9° à l'article 475 du même Code;	**25°** à l'article 475 du même Code ;
10° au livre II, titre IX, chapitre Ier, section 2bis, et chapitre Ierbis du même Code;	**26°** au livre II, titre IX, chapitre Ier, section 2bis, et chapitre Ierbis du même Code ;
10°bis. A l'article 504bis et 504ter du même Code;	**27°** aux articles 504bis et 504ter du même Code ;
10°ter. A l'article 504quater du même Code.	**28°** à l'article 504quater du même Code ;
11° à l'article 505, alinéa premier, 2°, 3° et 4° du même Code;	**29° à l'article 505, alinéa 1er, 1° du même Code lorsque les choses concernées ont été enlevées, détournées ou obtenues à l'aide d'un crime ou d'un délit visés au présent article;** **30°** à l'article 505, alinéa premier, 2°, 3° et 4°

	du même Code;
12° aux articles 510, 511, alinéa premier ou 516 du même Code;	**31°** aux articles 510, 511, alinéa 1er, ou 516 du même Code ;
13° à l'article 520 du même Code, si les circonstances visées par les articles 510 ou 511, alinéa premier, du même Code sont réunies;	**32°** à l'article 520 du même Code, si les circonstances visées aux articles 510 ou 511, alinéa 1er, du même Code sont réunies ;
13°bis Aux articles 550bis et 550ter du même Code;	**33°** aux articles 550bis et 550ter du même Code ;
14° à l'article 2bis, § 3, b ou § 4, b, de la loi du 24 février 1921 concernant le trafic des substances vénéneuses, soporifiques, stupéfiantes, désinfectantes ou antiseptiques;	**34°** à l'article 2bis de la loi du 24 février 1921 concernant le trafic des substances vénéneuses, soporifiques, stupéfiantes, psychotropes, désinfectantes ou antiseptiques **et des substances pouvant servir à la fabrication illicite de substances stupéfiantes et psychotropes** ;
15° à l'article 145, § 3 et § 3bis de la loi du 13 juin 2005 relative aux communications électroniques;	**35°** à l'article 145, §§ 3 et 3bis, de la loi du 13 juin 2005 relative aux communications électroniques ;
16° à l'article 10 de la loi du 5 août 1991 relative à l'importation, à l'exportation et au transit d'armes, de munitions et de matériel devant servir spécialement à un usage militaire et de la technologie y afférente.	**36°** à l'article 10 de la loi du 5 août 1991 relative à l'importation, à l'exportation et au transit d'armes, de munitions et de matériel devant servir spécialement à un usage militaire et de la technologie y afférente ;
16° bis à l'article 47 du décret du Parlement flamand du 15 juin 2012 concernant l'importation, l'exportation, le transit et le transfert de produits liés à la défense, d'autre matériel à usage militaire, de matériel de maintien de l'ordre, d'armes à feu civiles, de pièces et de munitions;	**37°** à l'article 47 du décret du parlement flamand du 15 juin 2012 concernant l'importation, l'exportation, le transit et le transfert de produits liés à la défense, d'autre matériel à usage militaire, de matériel de maintien de l'ordre, d'armes à feu civiles, de pièces et de munitions;
16° ter à l'article 20 du décret de la Région wallonne du 21 juin 2012 relatif à l'importation, à l'exportation, au transit et au transfert d'armes civiles et de produits liés à la défense;	**38°** à l'article 20 du décret de la Région wallonne du 21 juin 2012 relatif à l'importation, à l'exportation, au transit et au transfert d'armes civiles et de produits liés à la défense;
16° quater à l'article 42 de l'ordonnance de la Région de Bruxelles-Capitale du 20 juin 2013 relative à l'importation, à l'exportation, au transit et au transfert de produits liés à la défense, d'autre matériel pouvant servir à un usage militaire, de matériel lié au maintien de l'ordre, d'armes à feu à usage civil, de leurs pièces, accessoires et munitions;	**39°** à l'article 42 de l'ordonnance de la Région de Bruxelles-Capitale du 20 juin 2013 relative à l'importation, à l'exportation, au transit et au transfert de produits liés à la défense, d'autre matériel pouvant servir à un usage militaire, de matériel lié au maintien de l'ordre, d'armes à feu à usage civil, de leurs pièces, accessoires et munitions ;

16° quinquies aux articles 8 à 11, 14, 16, 19, 1°, 2°, 3°, 5° et 6°, 20, 22, 27 et 33 de la loi du 8 juin 2006 réglant des activités économiques et individuelles avec des armes, aussi appelée "Loi sur les armes";	**40°** aux articles 8 à 11, 14, 16, 19, 1°, 2°, 3°, 5° et 6°, 20, 22, 27 et 33 de la loi du 8 juin 2006 réglant des activités économiques et individuelles avec des armes, aussi appelée « Loi sur les armes »;
16° sexies à la loi du 28 mai 1956 relative aux substances et mélanges explosibles ou susceptibles de déflagrer et aux engins qui en sont chargés;	**41°** à la loi du 28 mai 1956 relative aux substances et mélanges explosibles ou susceptibles de déflagrer et aux engins qui en sont chargés ;
16° septies aux articles 21 à 26 de l'Accord de Coopération du 2 mars 2007 entre l'Etat fédéral, la Région flamande, la Région wallonne et la Région de Bruxelles-Capitale relatif à l'exécution de la Convention sur l'interdiction de la mise au point, de la fabrication, du stockage et de l'emploi des armes chimiques et sur leur destruction, faite à Paris le 13 janvier 1993;	**42°** aux articles 21 à 26 de l'Accord de Coopération du 2 mars 2007 entre l'Etat fédéral, la Région flamande, la Région wallonne et la Région de Bruxelles-Capitale relatif à l'exécution de la Convention sur l'interdiction de la mise au point, de la fabrication, du stockage et de l'emploi des armes chimiques et sur leur destruction, faite à Paris le 13 janvier 1993 ;
17° aux articles 77ter, 77quater et 77quinquies de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers;	**43**° aux articles **77bis à** 77quinquies de la loi du 15 décembre 1980 concernant l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers ;
18° à l'article 10, § 1er, 2°, de la loi du 15 juillet 1985 relative à l'utilisation de substances à effet hormonal, à effet anti-hormonal, à effet bêta-adrénergique ou à effet stimulateur de production chez les animaux;	**44**° à l'article 10, § 1er, 2°, de la loi du 15 juillet 1985 relative à l'utilisation de substances à effet hormonal, à effet antihormonal, à effet bêta-adrénergique ou à effet stimulateur de production chez les animaux ;
19° à l'article 1er de l'arrêté royal du 12 avril 1974 relatif à certaines opérations concernant les substances à action hormonale, anti-hormonale, anabolisante, anti-infectieuse, anti-parasitaire et anti-inflammatoire, l'article précité visant des infractions punies conformément à la loi du 24 février 1921 concernant le trafic des substances vénéneuses, soporifiques, stupéfiantes, désinfectantes ou antiseptiques;	**45**° article 1er de l'arrêté royal du 12 avril 1974 relatif à certaines opérations concernant les substances à action hormonale, antihormonale, anabolisante, bêta-adrénergique, anti-infectieuse, antiparasitaire et anti-inflammatoire, article précité visant des infractions punies conformément à la loi du 24 février 1921 concernant le trafic des substances vénéneuses, soporifiques, stupéfiantes, désinfectantes ou antiseptiques ;
§ 3. La tentative de commettre un crime visé au paragraphe précédent peut également justifier une mesure de surveillance.	§ 3. La tentative de commettre un crime visé au paragraphe précédent peut également justifier une mesure.
§ 4. Une infraction, visée aux articles 322 ou 323 du Code pénal, peut également justifier une mesure de surveillance, pour autant que l'association soit formée dans le but de commettre un attentat contre les personnes	§ 4. Une infraction, visée aux articles 322 ou 323 du Code pénal, peut également justifier une mesure, pour autant que l'association soit formée dans le but de commettre un attentat contre les personnes ou les

ou les propriétés visées au § 2 ou de commettre le fait punissable visé à l'article 467, alinéa 1er, du Code pénal.	propriétés visées au § 2 ou de commettre le fait punissable visé à l'article 467, alinéa 1er, du Code pénal.
§ 5. En cas de flagrant délit et tant que la situation de flagrant délit perdure, le procureur du Roi peut ordonner la mesure visée au § 1er pour les infractions visées à l'article 347bis ou 470 du Code pénal.	§ 5. En cas de flagrant délit et tant que la situation de flagrant délit perdure, le procureur du Roi peut ordonner la mesure visée au § 1er pour les infractions visées **aux articles 347bis, 434 ou 470** du Code pénal.
§ 6. Une autorité étrangère compétente peut, dans le cadre d'une enquête pénale, temporairement écouter, prendre connaissance et enregistrer, pendant leur transmission, des télécommunications privées lorsque la personne visée par cette mesure se trouve sur le territoire belge et si les conditions suivantes sont réunies :	§ 6. Une autorité étrangère compétente peut, dans le cadre d'une enquête pénale, temporairement **intercepter**, prendre connaissance et enregistrer **des communications non accessibles au public ou des données d'un système informatique** lorsque la personne visée par cette mesure se trouve sur le territoire belge et si les conditions suivantes sont réunies :
1° cette mesure n'implique pas l'intervention technique d'un acteur situé en Belgique; 2° l'autorité étrangère concernée a notifié cette mesure à une autorité judiciaire belge; 3° cette possibilité est prévue par un instrument de droit international liant la Belgique et l'Etat requérant; 4° la décision du juge d'instruction visée au § 7 n'a pas encore été communiquée à l'autorité étrangère concernée.	1° cette mesure n'implique pas l'intervention technique d'un acteur situé en Belgique ; 2° l'autorité étrangère concernée a notifié cette mesure à une autorité judiciaire belge ; 3° cette possibilité est prévue par un instrument de droit international liant la Belgique et l'État requérant ; 4° la décision du juge d'instruction visée au § 7 n'a pas encore été communiquée à l'autorité étrangère concernée.
Les données collectées en application du présent paragraphe ne peuvent être utilisées que si l'autorité judiciaire belge compétente autorise la mesure.	Les données collectées en application du présent paragraphe ne peuvent être utilisées que si l'autorité judiciaire belge compétente autorise la mesure.
§ 7. Dès que le procureur du Roi reçoit la notification visée au § 6, alinéa 1er, 2°, il en saisit sans délai le juge d'instruction.	§ 7. Dès que le procureur du Roi reçoit la notification visée au § 6, alinéa 1er, 2°, il en saisit sans délai le juge d'instruction.
Le juge d'instruction saisi d'une notification visée au paragraphe 6, alinéa 1er, 2°, autorise la mesure en question si celle-ci est recevable au regard des dispositions du présent article.	Le juge d'instruction saisi d'une notification visée au § 6, alinéa 1er, 2°, autorise la mesure en question si celle-ci est recevable au regard des dispositions du présent article.
Il notifie à l'autorité étrangère concernée sa décision dans les nonante-six heures suivant la réception de celle-ci par l'autorité judiciaire belge.	Il notifie à l'autorité étrangère concernée sa décision dans les nonante-six heures suivant la réception de celle-ci par l'autorité judiciaire belge.
Lorsqu'un délai supplémentaire est nécessaire, le juge d'instruction peut reporter de huit jours au maximum sa décision et la notification de celle-ci à l'autorité étrangère	Lorsqu'un délai supplémentaire est nécessaire, le juge d'instruction peut reporter de huit jours au maximum sa décision et la notification de celle-ci à l'autorité étrangère

compétente. Il en informe sans délai l'autorité étrangère compétente en indiquant les raisons de ce report. Si le juge d'instruction n'autorise pas la mesure visée au § 6, il informe également l'autorité étrangère que les données interceptées doivent être détruites sans pouvoir être utilisées.	compétente. Il en informe sans délai l'autorité étrangère compétente en indiquant les raisons de ce report. Si le juge d'instruction n'autorise pas la mesure visée au § 6, il informe également l'autorité étrangère que les données interceptées doivent être détruites sans pouvoir être utilisées.
Article 90quater	**Article 90quater**
§ 1. Toute mesure de surveillance sur la base de l'article 90ter est préalablement autorisée par une ordonnance motivée du juge d'instruction, que celui-ci communique au procureur du Roi. L'ordonnance est datée et indique : 1° les indices ainsi que les faits concrets et propres à la cause qui justifient la mesure conformément à l'article 90ter; 2° les motifs pour lesquels la mesure est indispensable à la manifestation de la vérité; 3° la personne, le moyen de communication ou de télécommunication ou le lieu soumis à la surveillance; 4° la période pendant laquelle la surveillance peut être pratiquée et qui ne peut excéder un mois à compter de la décision ordonnant la mesure; 5° les nom et qualité de l'officier de police judiciaire commis pour l'exécution de la mesure. § 2. Si la mesure comporte une opération sur un réseau de communication, l'opérateur de ce réseau, ou le fournisseur du service de télécommunication, est tenu de prêter son concours technique, quand le juge	§ 1er. Toute **mesure** sur la base de l'article 90ter **fait l'objet d'une autorisation écrite préalable et motivée du juge d'instruction, que celui-ci communique au procureur du Roi.** L'**autorisation** est datée et indique : 1° les indices ainsi que les faits concrets et propres à la cause qui justifient la mesure conformément à l'article 90ter ; 2° les motifs pour lesquels la mesure est indispensable à la manifestation de la vérité ; 3° la personne, le moyen de communication, le système informatique ou le lieu soumis à la surveillance ; 4° **la période pendant laquelle la mesure peut être exécutée et qui ne peut excéder un mois. Ce délai commence à courir le jour de l'autorisation ordonnant ou, dans le cas de l'article 90quinquies, alinéa 1er, prolongeant la mesure et s'achève la veille du quantième du mois suivant ;** 5° les nom et qualité de l'officier ou des officiers de police judiciaire commis pour l'exécution de la mesure. **En cas d'urgence, l'autorisation peut être donnée verbalement. Elle doit être confirmée dans la forme prévue à l'alinéa 2 au plus tard dans les vingt-quatre heures.** § 2. **Afin de permettre la mesure visée à l'article 90ter, § 1er, le juge d'instruction peut requérir, directement ou par l'intermédiaire d'un service de police désigné par le Roi, le concours :**

d'instruction le requiert directement ou par l'intermédiaire d'un service de police désigné par le Roi.	- de l'opérateur d'un réseau de communications électroniques ; et - **de toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.**
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, 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 à dix mille francs.	Toute personne qui refuse de prêter son concours technique aux réquisitions visées aux alinéas précédents, concours dont les modalités sont fixées par le Roi, sur la proposition du ministre de la Justice et du ministre compétent pour les Télécommunications, **ou ne le prête pas en temps réel ou, le cas échéant, au moment précisé dans la réquisition,** est punie d'une amende de vingt-six francs à **vingt mille** francs.
§ 3. Le juge d'instruction ne peut commettre pour l'exécution de son ordonnance que des officiers de police judiciaire, lesquels peuvent néanmoins se faire assister par des agents de police judiciaire dont les noms sont préalablement communiqués au juge d'instruction. Les noms des agents de police judiciaire chargés de l'exécution de l'ordonnance visée à l'article 90ter, § 1er, alinéa 2, ne sont pas mentionnés dans le dossier judiciaire.	§ 3. Le juge d'instruction ne peut commettre pour l'exécution **de la mesure visée à l'article 90ter, § 1er,** que des officiers de police judiciaire. **Ceux-ci** peuvent néanmoins se faire assister par des agents de police judiciaire **et, selon les conditions fixées par le Roi, par des agents du cadre administratif et logistique de la police intégrée. Ces dernières personnes ne peuvent être chargées de l'analyse du contenu des communications ou données enregistrées, sauf s'il s'agit d'une expertise spécifique, ou de la sélection des parties estimées pertinentes pour l'instruction, comme prévu à l'article 90sexies, § 1er, 2°.** **Les officiers de police judiciaire conservent les noms des personnes qui peuvent les assister dans une liste établie**

	séparément pour chaque dossier selon les modalités fixées par le Roi, après avis de la Commission pour la protection de la vie privée. Si ces personnes sont chargées de l'exécution de l'ordonnance visée à l'article 90ter, § 1er, alinéa 3, leur nom n'est pas mentionné dans le dossier judiciaire.
Les officiers de police judiciaire commis font rapport par écrit au moins tous les cinq jours au juge d'instruction sur l'exécution de l'ordonnance.	Les officiers de police judiciaire commis font rapport par écrit au moins tous les cinq jours au juge d'instruction sur l'exécution de l'ordonnance.
§ 4. Le juge d'instruction peut ordonner directement ou par l'intermédiaire d'un service de police désigné par le Roi, aux personnes dont il présume qu'elles ont une connaissance particulière du service de télécommunications qui fait l'objet d'une mesure de surveillance ou des services qui permettent de protéger ou de crypter les données qui sont stockées, traitées ou transmises par un système informatique, de fournir des informations sur le fonctionnement de ce système et sur la manière d'accéder au contenu de la télécommunication qui est ou a été transmise, dans une forme compréhensible.	§ 4. Le juge d'instruction peut **exiger, directement ou par le l'intermédiaire d'un service de police désigné par le Roi**, de personnes dont il présume qu'elles ont une connaissance particulière **du moyen de communication ou du système informatique** qui fait l'objet de la mesure ou de services ou applications qui permettent de protéger, **de coder** ou de crypter les données qui sont stockées, traitées ou transmises par **un moyen de communication ou** un système informatique, **qu'elles fournissent** des informations sur le fonctionnement de ce **moyen ou** système et sur la manière d'accéder à son contenu qui est ou a été transmis, dans une forme compréhensible.
Il peut ordonner aux personnes de rendre accessible le contenu de la télécommunication, dans la forme qu'il aura demandée. Ces personnes sont tenues d'y donner suite, dans la mesure de leurs moyens.	Il peut ordonner aux personnes de rendre accessible **ce** contenu, dans la forme qu'il aura souhaitée.
Celui qui refuse de fournir la collaboration ordonnée conformément aux alinéas précédents, est puni d'un emprisonnement de six mois à un an et d'une amende de vingt-six francs à vingt mille francs ou d'une de ces peines seulement.	**Toute personne qui refuse de prêter son concours technique aux réquisitions visées aux alinéas précédents** est punie d'un emprisonnement de six mois à un an et d'une amende de vingt-six francs à vingt mille francs ou d'une de ces peines seulement.
Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou est appelée à y prêter son concours technique, est liée par le secret de l'instruction. Toute violation du secret sera punie conformément à l'article 458 du Code pénal.	Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou **est requise d'**y prêter son concours technique, est **tenue au secret**. Toute violation du secret est punie conformément à l'article 458 du Code pénal.
	§ 5. Le cas échéant, l'article 39bis, § 3,

	alinéa 4, est applicable aux données recueillies par une recherche dans un système informatique en application de l'article 90ter, § 1er.
Article 90quinquies	**Article 90quinquies**
Le juge d'instruction peut prolonger une ou plusieurs fois les effets de son ordonnance pour un nouveau terme qui ne peut dépasser un mois, avec un maximum de six mois, sans préjudice de sa décision de mettre fin à la mesure dès que les circonstances qui l'ont justifiée ont disparu.	Le juge d'instruction peut prolonger une ou plusieurs fois les effets de son **autorisation visée à l'article 90quater, § 1er,** pour un nouveau terme qui ne peut dépasser un mois, avec un maximum de six mois, sans préjudice de sa décision de mettre fin à la mesure dès que les circonstances qui l'ont justifiée ont disparu. **Ce délai de six mois commence à courir le jour de la première autorisation ordonnant la mesure et s'achève la veille du quantième du sixième mois suivant. Si la mesure, en raison de sa préparation technique, a effectivement débuté un jour postérieur à celui de la première autorisation, ce délai de six mois commence à courir au moment de ce début effectif et au plus tard deux mois après le jour de la première autorisation.**
Les dispositions contenues dans l'article 90quater, § 1, sont applicables à la prolongation visée à l'alinéa précédent. L'ordonnance indique en outre les circonstances précises qui justifient la prolongation de la mesure. Si des circonstances nouvelles et graves nécessitent les mesures visées à l'article 90ter, le juge d'instruction peut ordonner une nouvelle mesure en observant les formalités définies aux articles 90ter et 90quater; dans ce cas, l'ordonnance doit mentionner les circonstances précises nouvelles et graves qui nécessitent et justifient une nouvelle mesure.	Les dispositions contenues dans l'article 90quater, § 1er, sont applicables à la prolongation visée à l'alinéa précédent. L'**autorisation** indique en outre les circonstances précises qui justifient la prolongation de la mesure. Si des circonstances nouvelles et graves nécessitent les mesures visées à l'article 90ter, le juge d'instruction peut ordonner une nouvelle mesure en observant les formalités définies aux articles 90ter et 90quater. Dans ce cas, l'**autorisation** indique en outre les circonstances précises qui justifient la prolongation de la mesure.
Article 90sexies	**Article 90sexies**
§ 1er. Les officiers de police judiciaire commis mettent à la disposition du juge d'instruction : 1° le fichier contenant les enregistrements effectués à la suite des mesures prises en application des articles 90ter, 90quater et	§ 1er. Les officiers de police judiciaire commis mettent à la disposition du juge d'instruction : 1° le fichier contenant les **communications non accessibles au public ou les données d'un système informatique enregistrées**

90quinquies;	**et obtenues** à la suite des mesures prises en application des articles 90ter, 90quater et 90quinquies ;
2° la transcription des passages des communications et télécommunications estimés pertinents pour l'instruction par les officiers de police judiciaire commis, et leur traduction éventuelle;	2° la transcription **ou reproduction** des parties des communications ou **données enregistrées** estimées pertinentes pour l'instruction par les officiers de police judiciaire commis, et leur traduction éventuelle ; 3° **le cas échéant, l'endroit où se trouvent les données visées au 2° dans le système informatique ;**
3° la simple indication des sujets abordés et des données d'identification des moyens de communication utilisés en ce qui concerne les communications ou télécommunications estimées non pertinentes.	**4° Une description générale** du **contenu** et des données d'identification des moyens de communication **ou systèmes informatiques** utilisés en ce qui concerne les communications ou **données** estimées non pertinentes.
§ 2. Sans préjudice de la sélection par les officiers de police judiciaire visés au paragraphe 1er, le juge d'instruction apprécie parmi toutes les communications ou télécommunications recueillies, les passages qui sont pertinents pour l'instruction. Dans la mesure où ces passages des communications ou télécommunications n'ont pas été transcrits ou traduits conformément au paragraphe 1er, ils seront transcrits et traduits à titre additionnel. Le juge d'instruction en fait dresser procès-verbal.	**§ 2.** Sans préjudice de la sélection par les officiers de police judiciaire visés au § 1er, le juge d'instruction apprécie parmi toutes les **communications non accessibles au public ou données d'un système informatique** qui ont été enregistrées les parties qui sont pertinentes pour l'instruction. Dans la mesure où ces **parties** de communications ou données n'ont pas été transcrites, **reproduites** ou traduites conformément **au § 1er**, elles seront transcrites, **reproduites et éventuellement** traduites. Le juge d'instruction en fait dresser procès-verbal.
§ 3. Les communications ou télécommunications qui sont couvertes par le secret professionnel ne sont pas consignées dans le procès-verbal. Ces communications ou télécommunications sont déposées au greffe dans un fichier sous pli scellé. S'il s'agit de personnes visées à l'article 90octies, alinéa 1er, il est procédé conformément à l'article 90octies, alinéa 2.	§ 3. Les communications **non accessibles au public** ou **données d'un système informatique** qui sont couvertes par le secret professionnel ne sont pas consignées dans le procès-verbal. Ces communications ou **données** sont déposées au greffe dans un fichier sous pli scellé. S'il s'agit de personnes visées à l'article **90octies**, on procède ainsi qu'il est prévu **à cet article**.
§ 4. Les ordonnances du juge d'instruction, les rapports des officiers de police judiciaire visés à l'article 90quater, § 3, et les procès-verbaux relatifs à l'exécution de la mesure, sont joints au dossier au plus tard après qu'il soit mis fin à la mesure.	§ 4. Les **autorisations** du juge d'instruction, les rapports des officiers de police judiciaire visés à l'article 90quater, § 3, et les procès-verbaux relatifs à l'exécution de la mesure, sont joints au dossier au plus tard après qu'il **est** mis fin à la mesure.

Article 90septies	**Article 90septies**
Les communications ou télécommunications recueillies grâce aux mesures prises en application des articles 90ter, 90quater et 90quinquies, sont enregistrées. L'objet de la mesure ainsi que les jours et heures auxquels celle-ci a été exécutée sont enregistrés au début et à la fin de chaque enregistrement qui s'y rapporte.	**§ 1er. Les moyens appropriés sont utilisés pour garantir l'intégrité et la confidentialité des communications non accessibles au public ou données d'un système informatique qui ont été enregistrées.** **§ 2. Chaque fichier contient le sujet des communications non accessibles au public ou données d'un système informatique qui ont été enregistrées ainsi que les jours et heures auxquels la mesure a été exécutée.**
A l'exception de la transcription des passages de l'enregistrement des communications et télécommunications estimés pertinents avec traduction éventuelle et de l'indication des sujets abordés et des données d'identification des moyens de télécommunication à partir desquels ou vers lesquels il a été appelé en ce qui concerne les communications et télécommunications estimées non pertinentes, toute note prise dans le cadre de l'exécution des mesures visées à l'alinéa précédent par les personnes commises à cette fin qui n'est pas consignée dans un procès-verbal, est détruite. L'officier de police judiciaire commis pour l'exécution de la mesure procède à cette destruction et en fait mention dans un procès-verbal.	**§ 3.** Toute note prise dans le cadre de l'exécution des mesures visées **aux articles 90ter, 90quater et 90quinquies** par les personnes commises à cette fin qui n'est pas consignée dans un procès-verbal, est détruite, à l'exception de **ce qui est mentionné à l'article 90sexies, § 1er, 2°, 3° et 4°, et sans préjudice de l'article 33 de la loi du XXX relative à l'amélioration des méthodes particulières de recherche et de quelques autres méthodes d'enquête**. Le**s** officier**s** de police judiciaire commis pour l'exécution de la mesure procèd**ent** à cette destruction et en **font** mention dans un procès-verbal. **Pour des raisons de gestion et en vue du respect de l'obligation de l'article 90decies, les données administratives strictement nécessaires peuvent néanmoins être conservées au sein du service désigné par le Roi.**
Les enregistrements accompagnés de la transcription des passages de l'enregistrement des communications et télécommunications estimés pertinents avec traduction éventuelle, de l'indication des sujets abordés et des données d'identification des moyens de télécommunication à partir desquels ou vers lesquels il a été appelé en ce qui concerne les communications et télécommunications estimées non pertinentes, et des copies des procès-verbaux sont conservés au greffe sous pli scellé.	**§ 4. Les fichiers visés à l'article 90sexies, § 1er, 1°, sont conservés au greffe sous pli scellé. Ils peuvent en outre être conservés au sein du service désigné par le Roi aux conditions et modalités fixées par Lui** après avis de la Commission de la protection de la vie privée. **Les pièces visées à l'article 90sexies, § 1er, 2°, 3° et 4°, et les copies des procès-verbaux sont conservées au greffe sous pli scellé.**
Le greffier mentionne dans un registre spécial tenu journellement :	**§ 5.** Le greffier mentionne dans un registre spécial tenu journellement :

1° le dépôt de chaque enregistrement, ainsi que de la transcription des passages de l'enregistrement des communications et télécommunications estimés pertinents avec traduction éventuelle et de l'indication des sujets abordés et des données d'identification des moyens de télécommunication à partir desquels ou vers lesquels il a été appelé en ce qui concerne les communications et télécommunications estimées non pertinentes;	1° le **jour du** dépôt **des fichiers et pièces visés à l'article 90sexies, § 1er, ainsi que de chaque copie de procès-verbal** ;
2° le dépôt de chaque copie de procès-verbal;	
3° le jour de leur dépôt;	
4° le nom du juge d'instruction qui a ordonné ou confirmé la mesure et l'objet de celle-ci;	2° le nom du juge d'instruction qui a ordonné ou confirmé la mesure et l'objet de celle-ci ;
5° le jour où les scellés sont ouverts et éventuellement réapposés;	3° le jour où les scellés sont ouverts et éventuellement réapposés ;
6° la date de prise de connaissance de l'enregistrement, de la transcription des passages de l'enregistrement des communications et télécommunications estimés pertinents avec traduction éventuelle et l'indication des sujets abordés et des données d'identification des moyens de télécommunication à partir desquels ou vers lesquels il a été appelé en ce qui concerne les communications et télécommunications estimées non pertinentes, ou des copies des procès-verbaux, ainsi que le nom des personnes qui en ont pris connaissance;	4° la date de prise de connaissance **des fichiers et pièces visés à l'article 90sexies, § 1er,** des copies des procès-verbaux, ainsi que le nom des personnes qui en ont pris connaissance ;
7° tous les autres événements qui s'y rapportent.	5° tous les autres événements qui s'y rapportent.
Les moyens appropriés sont utilisés pour garantir l'intégrité et la confidentialité de la communication ou de la télécommunication enregistrée et, dans la mesure du possible, pour réaliser sa transcription ou sa traduction. La même règle vaut pour la conservation au greffe des enregistrements et de leur transcription ou de leur traduction et pour les mentions dans le registre spécial. Le Roi détermine, après avoir recueilli l'avis de la Commission de la protection de la vie privée, ces moyens et le moment où ils remplacent la conservation sous pli scellé ou le registre spécial prévus aux alinéas 3 et 4.	**§ 6.** L'inculpé, le prévenu, la partie civile ou leurs conseils reçoivent, sur simple demande, copie de la totalité des **communications non accessibles au public ou données d'un système informatique**, dont certaines **parties** estimées pertinentes ont été transcrites **ou reproduites** et consignées dans un procès-verbal qu'ils ont le droit de consulter. **L'inculpé, le prévenu, la partie civile ou leurs conseils peuvent demander au juge d'instruction de consulter au greffe les autres fichiers ou pièces déposés**

L'inculpé, le prévenu, la partie civile, la partie civilement responsable ou leurs conseils reçoivent, sur simple demande, copie de la totalité de l'enregistrement des communications et télécommunications dont certains passages estimés pertinents ont été transcrits et consignés dans un procès-verbal qu'ils ont le droit de consulter. Le juge se prononce sur la demande de l'inculpé, du prévenu, de la partie civile ou de leurs conseils, de consulter la totalité ou des parties des autres enregistrements et des transcriptions déposés au greffe qui ne sont pas consignées dans un procès-verbal, et sur leur demande de transcrire des parties additionnelles des enregistrements. La demande qui est adressée au juge d'instruction est traitée conformément à l'article 61quinquies. Le juge d'instruction peut en outre rejeter cette demande pour des raisons liées à la protection d'autres droits ou intérêts des personnes. Sans préjudice des alinéas précédents, le juge se prononce sur la demande de l'inculpé, du prévenu, de la partie civile ou de leurs conseils de consulter les parties des enregistrements déposés au greffe de communications ou de télécommunications privées auxquelles la personne concernée a participé et qui ne sont pas transcrites et consignées dans un procès-verbal, et sur leur demande de transcrire des parties additionnelles de ces enregistrements.	**conformément au § 4 au greffe, ainsi que de transcrire ou reproduire des parties supplémentaires des communications ou données enregistrées. La demande, adressée au juge d'instruction, est traitée conformément à l'article 61quinquies.** **Le juge d'instruction peut en outre rejeter cette demande s'il estime que la consultation, la transcription ou la reproduction des parties supplémentaires n'est pas nécessaire à la manifestation de la vérité, s'il le juge à ce moment préjudiciable à l'enquête ou pour des raisons liées à la protection d'autres droits ou intérêts de personnes. Il peut également limiter la consultation ou la transcription ou reproduction de parties supplémentaires à une sélection de fichiers ou pièces qu'il détermine.**
Article 90octies	**Article 90octies**
La mesure ne pourra porter sur les locaux utilisés à des fins professionnelles, la résidence ou les moyens de communication ou de télécommunication d'un avocat ou d'un médecin que si celui-ci est lui-même soupçonné d'avoir commis une des infractions visées à l'article 90ter ou d'y avoir participé, ou si des faits précis laissent présumer que des tiers soupçonnés d'avoir commis une des infractions visées à l'article 90ter, utilisent ses locaux, sa résidence ou ses moyens de communication ou de télécommunication.	**§ 1er.** La mesure ne pourra porter sur les locaux utilisés à des fins professionnelles, la résidence, les moyens de communication **ou les systèmes informatiques** d'un avocat ou d'un médecin que si celui-ci est lui-même soupçonné d'avoir commis une des infractions visées à l'article 90ter ou d'y avoir participé, ou si des faits précis laissent présumer que des tiers soupçonnés d'avoir commis une des infractions visées à l'article 90ter, utilisent ses locaux, sa résidence, ses moyens de communication **ou ses systèmes informatiques**.

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 des communications ou télécommunications recueillies qu'il estime relever du secret professionnel et qui ne seront pas consignés au procès-verbal conformément à l'article 90sexies, troisième alinéa	**§ 2.** 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 personnes sont tenues au secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.** **§ 3. Le juge d'instruction évalue, après concertation avec le bâtonnier ou le représentant de l'ordre provincial des médecins, quelles parties des communications non accessibles au public ou données d'un système informatique visées à l'article 90sexies, § 3, qu'il estime pertinentes pour l'instruction, relèvent du secret professionnel et quelles sont celles qui n'en relèvent pas.** **Seules les parties des communications ou données visées à l'alinéa précédent qui sont estimées ne pas relever du secret professionnel sont transcrites ou reproduites et, le cas échéant, traduites. Le juge d'instruction en fait dresser procès-verbal. Les fichiers contenant ces communications ou données sont déposés au greffe sous pli scellé.** **Toutes les autres communications ou données sont déposées au greffe dans un autre fichier sous pli scellé séparé.**
Article 90novies	**Article 90novies**
Au plus tard quinze jours après le moment où la décision sur le règlement de la procédure est devenue définitive ou après que la citation visée à l'article 524bis , § 6, a été déposée au greffe du tribunal ou de la cour, le greffier avise par écrit, sur réquisition du procureur du Roi ou, le cas échéant, du procureur général, toute personne ayant fait l'objet d'une mesure visée par l'article 90ter, de la nature de ladite mesure et des dates auxquelles elle a été exécutée.	Au plus tard quinze jours après le moment où la décision sur le règlement de la procédure est devenue définitive ou après que la citation visée à l'article 524bis, § 6, a été déposée au greffe du tribunal ou de la cour, le greffier avise par écrit, sur réquisition du procureur du Roi ou, le cas échéant, du procureur général, toute personne ayant fait l'objet d'une mesure visée par l'article 90ter, de la nature de ladite mesure et des dates auxquelles elle a été exécutée, **sauf si son identité ou son adresse ne peut être raisonnablement retrouvée.**
Article 90decies	**Article 90decies**

Le Ministre de la Justice fait rapport annuellement au Parlement sur l'application des articles 90ter à 90novies. 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. À 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.	Le ministre de la Justice fait rapport annuellement au Parlement sur l'application des articles 90ter à 90novies. 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, **46quinquies**, 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. À 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.
Article 235ter	**Article 235ter**
§ 1er. La chambre des mises en accusation est chargée de contrôler de la mise en oeuvre des méthodes particulières de recherche d'observation et d'infiltration. Dès la clôture de l'information dans laquelle ces méthodes ont été utilisées et avant que le ministère public ne procède à la citation directe, la chambre des mises en accusation examine, sur la réquisition du ministère public, la régularité des méthodes particulières de recherche d'observation et d'infiltration. Dès le moment où le juge d'instruction	§ 1er. La chambre des mises en accusation est chargée de contrôler la mise en œuvre des méthodes particulières de recherche d'observation et d'infiltration **et l'application de la mesure visée à l'article 46septies si un dossier confidentiel a été ouvert dans ce cadre.** Dès la clôture de l'information dans laquelle ces méthodes ont été utilisées et avant que le ministère public ne procède à la citation directe, la chambre des mises en accusation examine, sur la réquisition du ministère public, la régularité des méthodes particulières de recherche d'observation et d'infiltration **et de la mesure visée à l'article 46sexies**. Dès le moment où le juge d'instruction

communique son dossier au procureur du Roi en vertu de l'article 127, § 1er, alinéa 1er, la chambre des mises en accusation examine, sur la réquisition du ministère public, la régularité des méthodes particulières de recherche d'observation et d'infiltration qui ont été appliquées dans le cadre de l'instruction ou de l'information qui l'a précédée.	communique son dossier au procureur du Roi en vertu de l'article 127, § 1er, alinéa 1er, la chambre des mises en accusation examine, sur la réquisition du ministère public, la régularité des méthodes particulières de recherche d'observation et d'infiltration **et de la mesure visée à l'article 46sexies** qui ont été appliquées dans le cadre de l'instruction ou de l'information qui l'a précédée.
§ 2. La chambre des mises en accusation se prononce dans les trente jours de la réception de la réquisition du ministère public. Ce délai est ramené à huit jours si l'un des inculpés se trouve en détention préventive.	§ 2. La chambre des mises en accusation se prononce dans les trente jours de la réception de la réquisition du ministère public. Ce délai est ramené à huit jours si l'un des inculpés se trouve en détention préventive.
La chambre des mises en accusation entend, séparément et en l'absence des parties, le procureur général en ses observations.	La chambre des mises en accusation entend, séparément et en l'absence des parties, le procureur général en ses observations.
Elle entend séparément les parties civiles et les inculpés, en présence du procureur général], après convocation qui leur est notifiée par le greffier par télécopie ou par lettre recommandée à la poste au plus tard quarante-huit heures avant l'audience. Le greffier les informe également dans cette convocation, que le dossier répressif est mis à leur disposition au greffe, en original ou en copie pour consultation pendant cette période. [La chambre des mises en accusation peut décider que l'inculpé qui se trouve en détention préventive comparaîtra par vidéoconférence.]	Elle entend séparément les parties civiles et les inculpés, en présence du procureur général, après convocation qui leur est notifiée par le greffier par télécopie ou par lettre recommandée à la poste au plus tard quarante-huit heures avant l'audience. Le greffier les informe également dans cette convocation, que le dossier répressif est mis à leur disposition au greffe, en original ou en copie pour consultation pendant cette période. [La chambre des mises en accusation peut décider que l'inculpé qui se trouve en détention préventive comparaîtra par vidéoconférence.]
Pour les méthodes particulières de recherche d'observation et d'infiltration, elle peut entendre, séparément et en l'absence des parties, le juge d'instruction et l'officier de police judiciaire visé aux articles 47sexies, § 3, 6°, et 47octies, § 3, 6°.	Pour les méthodes particulières de recherche d'observation et d'infiltration **et la mesure visée à l'article 46sexies**, elle peut entendre, séparément et en l'absence des parties, le juge d'instruction et l'officier de police judiciaire visé aux articles 47sexies, § 3, 6°, et 47octies, § 3, 6°, **et l'officier de police judiciaire chargé de diriger la mise en œuvre de la mesure visée à l'article 46sexies**.
La chambre des mises en accusation peut charger le juge d'instruction d'entendre les fonctionnaires de police chargés d'exécuter l'observation et l'infiltration et le civil visé à l'article 47octies, § 1er, alinéa 2, en application des articles 86bis et 86ter. Elle	La chambre des mises en accusation peut charger le juge d'instruction d'entendre les fonctionnaires de police chargés d'exécuter l'observation et l'infiltration, le civil visé à l'article 47octies, § 1er, alinéa 2, en application des articles 86bis et 86ter, **les**

peut décider d'être présente à l'audition menée par le juge d'instruction ou de déléguer un de ses membres à cet effet.	**fonctionnaires de police chargés de la mise en œuvre de la mesure visée à l'article 46sexies et le civil visé à l'article 46sexies, § 1er, alinéa 2**. Elle peut décider d'être présente à l'audition menée par le juge d'instruction ou de déléguer un de ses membres à cet effet.
§ 3. Le ministère public soumet au président de la chambre des mises en accusation le dossier confidentiel visé aux articles 47septies, § 1er, alinéa 2, ou 47novies, § 1er, alinéa 2, qui porte sur l'information ou sur l'instruction visée au § 1er. Seuls les magistrats de la chambre des mises en accusation ont le droit de consulter ce dossier confidentiel.	§ 3. Le ministère public soumet au président de la chambre des mises en accusation le dossier confidentiel visé aux articles **46sexies, § 3, alinéa 7,** 47septies, § 1er, alinéa 2, ou 47novies, § 1er, alinéa 2, qui porte sur l'information ou sur l'instruction visée au § 1er. Seuls les magistrats de la chambre des mises en accusation ont le droit de consulter ce dossier confidentiel.
Le président de la chambre des mises en accusation prend les mesures nécessaires en vue d'assurer la protection du dossier confidentiel. Il le restitue immédiatement au ministère public après en avoir pris connaissance.	Le président de la chambre des mises en accusation prend les mesures nécessaires en vue d'assurer la protection du dossier confidentiel. Il le restitue immédiatement au ministère public après en avoir pris connaissance.
§ 4. L'arrêt de la chambre des mises en accusation ne peut pas faire mention du contenu du dossier confidentiel, ni du moindre élément susceptible de compromettre les moyens techniques et les techniques d'enquête policière utilisés ou la garantie de la sécurité et de l'anonymat de l'indicateur, des fonctionnaires de police chargés de l'exécution de l'observation ou de l'infiltration et du civil visé à l'article 47octies, § 1er, alinéa 2.	§ 4. L'arrêt de la Cour de cassation ne peut pas faire mention du contenu du dossier confidentiel, ni du moindre élément susceptible de compromettre les moyens techniques et les techniques d'enquête policière utilisés ou la garantie de la sécurité et de l'anonymat de l'indicateur, des fonctionnaires de police chargés de la mise en œuvre de l'observation, **de** l'infiltration **ou de la mesure visée à l'article 46sexies, et** du civil visé **aux** articles 47octies, § 1er, alinéa 2, **et 46sexies, § 1er, alinéa 2**.
§ 5. Il est procédé pour le surplus conformément à l'article 235bis, §§ 5 et 6.	§ 5. Il est procédé pour le surplus conformément à l'article 235bis, §§ 5 et 6.
Article 235quater	**Article 235quater**
§ 1er. Sans préjudice de l'exercice du contrôle visé à l'article 235ter, la chambre des mises en accusation peut, à titre provisoire, d'office, à la demande du juge d'instruction ou sur la réquisition du ministère public examiner, pendant l'instruction, la régularité des méthodes particulières de recherche d'observation et d'infiltration qui ont été appliquées dans le cadre de cette	§ 1er. Sans préjudice de l'exercice du contrôle visé à l'article 235ter, la chambre des mises en accusation peut, à titre provisoire, d'office, à la demande du juge d'instruction ou sur la réquisition du ministère public examiner, pendant l'instruction, la régularité des méthodes particulières de recherche d'observation et d'infiltration **et de la mesure visée à l'article 46sexies si un**

instruction ou de l'information qui l'a précédée.	**dossier confidentiel a été ouvert dans ce cadre,** qui ont été appliquées dans le cadre de cette instruction ou de l'information qui l'a précédée.
Afin que la chambre des mises en accusation puisse exercer d'office son contrôle, les procureurs du Roi de son ressort informent systématiquement et immédiatement le président de la chambre des mises en accusation des dossiers pour lesquels des observations et des infiltrations ont été décidées par le ministère public ou par le juge d'instruction.	Afin que la chambre des mises en accusation puisse exercer d'office son contrôle, les procureurs du Roi de son ressort informent systématiquement et immédiatement le président de la chambre des mises en accusation des dossiers pour lesquels des observations et des infiltrations **et la mesure visée à l'article 46sexies, si un dossier confidentiel a été ouvert dans ce cadre, ont été décidées par le ministère public ou par le juge d'instruction**.
§ 2. La chambre des mises en accusation entend, séparément et en l'absence des parties, le procureur général en ses observations.	§ 2. La chambre des mises en accusation entend, séparément et en l'absence des parties, le procureur général en ses observations.
Pour les méthodes particulières de recherche d'observation ou d'infiltration, elle peut entendre, séparément et en l'absence des parties, le juge d'instruction et l'officier de police judiciaire visé aux articles 47sexies, § 3, 6°, et 47octies, § 3, 6°.	Pour les méthodes particulières de recherche d'observation ou d'infiltration **et la mesure visée à l'article 46sexies**, elle peut entendre, séparément et en l'absence des parties, le juge d'instruction et l'officier de police judiciaire visé aux articles 47sexies, § 3, 6°, et 47octies, § 3, 6°, **et l'officier de police judiciaire chargé de diriger la mise en œuvre de la mesure visée à l'article 46sexies**.
§ 3. Le ministère public soumet au président de la chambre des mises en accusation le dossier confidentiel visé aux articles 47septies, § 1er, alinéa 2, ou 47novies, § 1er, alinéa 2, qui porte sur l'instruction visée au § 1er. Seuls les magistrats de la chambre des mises en accusation ont le droit de consulter ce dossier confidentiel.	§ 3. Le ministère public soumet au président de la chambre des mises en accusation le dossier confidentiel visé aux articles 47septies, § 1er, alinéa 2, ou 47novies, § 1er, alinéa 2, **ou 46sexies, § 3, alinéa 7,** qui porte sur l'instruction visée au § 1er. Seuls les magistrats de la chambre des mises en accusation ont le droit de consulter ce dossier confidentiel.
Le président de la chambre des mises en accusation prend les mesures nécessaires en vue d'assurer la protection du dossier confidentiel. Il le restitue immédiatement au ministère public après en avoir pris connaissance.	Le président de la chambre des mises en accusation prend les mesures nécessaires en vue d'assurer la protection du dossier confidentiel. Il le restitue immédiatement au ministère public après en avoir pris connaissance.
§ 4. L'arrêt de la chambre des mises en accusation ne peut pas faire mention du contenu du dossier confidentiel, ni du moindre élément susceptible de	§ 4. L'arrêt de la Cour de cassation ne peut pas faire mention du contenu du dossier confidentiel, ni du moindre élément susceptible de compromettre les moyens

compromettre les moyens techniques et les techniques d'enquête policière utilisés ou la garantie de la sécurité et de l'anonymat de l'indicateur, des fonctionnaires de police chargés de l'exécution de l'observation ou de l'infiltration et du civil visé à l'article 47octies, § 1er, alinéa 2.	techniques et les techniques d'enquête policière utilisés ou la garantie de la sécurité et de l'anonymat de l'indicateur, des fonctionnaires de police chargés de la mise en œuvre de l'observation, **de** l'infiltration ou **de la mesure visée à l'article 46sexies, et** du civil visé **aux** articles 47octies, § 1er, alinéa 2, **et 46sexies, § 1er, aliéna 2**.
Article 464/13	**Article 464/13**
§ 1er. Le magistrat EPE ou le service de police requis peut, par décision écrite et motivée, requérir l'opérateur d'un réseau de communications électroniques ou le fournisseur d'un service de communications électroniques de lui communiquer les renseignements suivants :	§ 1er. Le magistrat EPE ou le service de police requis peut, par décision écrite et motivée, requérir les **acteurs visés à l'alinéa 2** de lui communiquer les renseignements suivants :
1° l'identification d'un abonné ou d'un utilisateur habituel d'un service de communications électroniques ou du moyen de communication électronique utilisé;	1° l'identification d'un abonné ou d'un utilisateur habituel d'un **service visé à l'alinéa 2, deuxième tiret,** ou bien du moyen de communication électronique utilisé ;
2° l'identification des services de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée.	2° l'identification des **services visés à l'alinéa 2, deuxième tiret,** auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée. **Les acteurs suivants sont tenus de collaborer conformément à l'alinéa précédent :** **- l'opérateur d'un réseau de communications électroniques ; et** **- toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.**
§ 2. Chaque opérateur d'un réseau de communications électroniques et chaque	§ 2. **Les acteurs visés au § 1er, alinéa 2, fournissent** tous les renseignements

fournisseur d'un service de communications électroniques communiquent tous les renseignements disponibles dans le délai et selon les modalités fixés par l'arrêté royal pris en exécution de l'article 46bis, § 2, alinéas 1er et 2.	disponibles **en temps réel ou, le cas échéant, au moment précisé dans la décision, selon les modalités** fixées par l'arrêté royal pris en exécution de l'article 46bis, § 2, alinéas 1er et 2.
Tout refus de communiquer les données est puni d'une amende de vingt-six euros à dix mille euros.	**Toute personne qui refuse de communiquer les données ou qui ne les communique pas en temps réel ou, le cas échéant, au moment précisé dans la réquisition** est punie d'une amende de vingt-six euros à dix mille euros.
§ 3. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours est tenue de garder le secret. Toute violation du secret sera punie conformément à l'article 458 du Code pénal.	§ 3. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal
Article 464/25	**Article 464/25**
§ 1er. Le magistrat EPE ou le service de police requis peut faire procéder, en requérant un opérateur d'un réseau de communication électronique ou le fournisseur d'un service de communication électronique :	§ 1er. Le magistrat EPE ou le service de police requis peut requérir **les acteurs visés à l'alinéa 2** de faire procéder :
1° au repérage des données d'appel de moyens de communication électronique à partir desquels ou vers lesquels des appels sont adressés ou ont été adressés;	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° à la localisation de l'origine ou de la destination de communications électroniques.	2° a la localisation de l'origine ou de la destination de télécommunications. **Les acteurs suivants sont tenus de collaborer conformément à l'alinéa précédent :** **- l'opérateur d'un réseau de communications électroniques ; et** **- toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser**

	des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.
Dans les cas visés à l'alinéa 1er, pour chaque moyen de communication électronique dont les données d'appel sont repérées ou pour lequel l'origine ou la destination de la communication électronique est localisée, le jour, l'heure, la durée et, si nécessaire, le lieu de la communication électronique sont indiqués et consignés dans un procès-verbal.	Dans les cas visés à l'alinéa 1er, pour chaque moyen de communication électronique dont les données d'appel sont repérées ou pour lequel l'origine ou la destination de la communication électronique est localisée, le jour, l'heure, la durée et, si nécessaire, le lieu de la communication électronique sont indiqués et consignés dans un procès-verbal.
Le magistrat EPE précise dans sa décision la durée pendant laquelle la mesure pourra s'appliquer, cette durée ne pouvant excéder, en ce qui concerne les futures données de communication électronique, deux mois à dater de l'ordonnance, sans préjudice de renouvellement.	Le magistrat EPE précise dans sa décision la durée pendant laquelle la mesure pourra s'appliquer, cette durée ne pouvant excéder, en ce qui concerne les futures données de communication électronique, deux mois à dater de l'ordonnance, sans préjudice de renouvellement.
§ 2. Chaque opérateur d'un réseau de communication électronique et chaque fournisseur d'un service de communication électronique communiquent les informations demandées dans un délai et selon les modalités fixées par l'arrêté royal pris en exécution de l'article 88bis, § 2, alinéas 1er et 3.	§ 2. **Les acteurs visés au § 1er, alinéa 2, communiquent** les renseignements requis **en temps réel ou, le cas échéant, au moment précisé dans la décision, selon les modalités** fixées par l'arrêté royal pris en exécution de l'article 88bis, § 2, alinéas 1er et 3.
Toute personne qui refuse de prêter son concours technique aux réquisitions visées dans le présent article est punie d'une amende de vingt-six euros à dix mille euros.	Toute personne qui **refuse** de prêter son concours technique aux réquisitions visées dans le présent article **ou ne le prête pas en temps réel ou, le cas échéant, au moment précisé dans la décision** est punie d'une amende de vingt-six euros à dix mille euros.
§ 3. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours est tenue de garder le secret.	§ 3. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret.
Toute violation du secret sera punie conformément à l'article 458 du Code pénal.	Toute violation du secret est punie conformément à l'article 458 du Code pénal.
CODE PENAL	**CODE PENAL**
LIVRE 2, TITRE IV, CHAPITRE VBIS – DES ECOUTES, DE LA PRISE DE CONNAISSANCE ET DE L'ENREGISTREMENT DE	**LIVRE 2, TITRE IV, CHAPITRE VBIS – INTERCEPTION, PRISE DE CONNAISSANCE ET ENREGISTREMENT DE COMMUNICATIONS NON**

COMMUNICATIONS ET DE TELECOMMUNICATIONS PRIVEES	**ACCESSIBLES AU PUBLIC ET DE DONNEES D'UN SYSTEME INFORMATIQUE**
Article 259bis	**Article 259bis**
§ 1. Sera puni d'un emprisonnement de six mois à deux ans et d'une amende de cinq cents euros à vingt mille euros ou d'une de ces peines seulement, tout officier ou fonctionnaire public, dépositaire ou agent de la force publique 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 :	§ 1er. Sera puni d'un emprisonnement de six mois à deux ans et d'une amende de cinq cents [euros] à vingt mille [euros] ou d'une de ces peines seulement, tout officier ou fonctionnaire public, dépositaire ou agent de la force publique 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 :
1° soit, intentionnellement, à l'aide d'un appareil quelconque, écoute ou fait écouter, prend connaissance ou fait prendre connaissance, enregistre ou fait enregistrer, pendant leur transmission, des communications ou des télécommunications privées, auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications ou télécommunications;	1° soit, intentionnellement, à l'aide d'un appareil quelconque, **intercepte ou fait intercepter**, prend connaissance ou fait prendre connaissance, enregistre ou fait enregistrer des **communications non accessibles au public**, auxquelles il ne prend pas part, sans le consentement de tous les participants à ces **communications** ;
2° soit, avec l'intention de commettre une des infractions mentionnées ci-dessus, installe ou fait installer un appareil quelconque;	2° soit, avec l'intention de commettre une des infractions mentionnées ci-dessus, installe ou fait installer un appareil quelconque ;
3° soit, sciemment, détient, révèle ou divulgue à une autre personne le contenu de communications ou de télécommunications privées, illégalement écoutées ou enregistrées, ou dont il a pris connaissance illégalement, ou utilise sciemment d'une manière quelconque une information obtenue de cette façon.	3° soit, sciemment, **détient, révèle ou divulgue à une autre personne le contenu de communications non accessibles au public ou de données d'un système informatique illégalement interceptées ou enregistrées**, ou dont il a pris connaissance illégalement, ou utilise sciemment d'une manière quelconque une information obtenue de cette façon.
§ 2. Sera puni d'un emprisonnement de six mois à trois ans et d'une amende de cinq cents euros à trente mille euros ou d'une de ces peines seulement, tout officier ou fonctionnaire public, dépositaire ou agent de la force publique 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, utilise un enregistrement, légalement effectué, de communications ou de télécommunications	§ 2. Sera puni d'un emprisonnement de six mois à trois ans et d'une amende de cinq cents [euros] à trente mille [euros] ou d'une de ces peines seulement, tout officier ou fonctionnaire public, dépositaire ou agent de la force publique 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, utilise **un enregistrement, légalement effectué, de communications non accessibles au**

privées.	**public ou de données d'un système informatique**.
§ 2bis. Sera puni d'un emprisonnement de six mois à deux ans et d'une amende de cinq cents euros à vingt mille euros ou d'une de ces peines seulement, tout officier ou fonctionnaire public, dépositaire ou agent de la force publique 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, indûment, possède, produit, vend, obtient en vue de son utilisation, importe, diffuse ou met à disposition sous une autre forme un dispositif, y compris des données informatiques, principalement conçu ou adapté pour permettre la commission de l'infraction prévue au § 1er.	§ 2bis. Sera puni d'un emprisonnement de six mois à deux ans et d'une amende de cinq cents euros à vingt mille euros ou d'une de ces peines seulement, tout officier ou fonctionnaire public, dépositaire ou agent de la force publique 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, indûment, possède, produit, vend, obtient en vue de son utilisation, importe, diffuse ou met à disposition sous une autre forme un dispositif, y compris des données informatiques, principalement conçu ou adapté pour permettre la commission de l'infraction prévue au § 1er.
§ 3. La tentative de commettre une des infractions visées aux §§ 1er, 2 ou 2bis est punie comme l'infraction elle-même.	§ 3. La tentative de commettre une des infractions visées aux §§ 1er et 2 est punie comme l'infraction elle-même.
§ 4. Les peines prévues aux §§ 1er à 3 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans à compter du prononcé d'un jugement ou d'un arrêt, passés en force de chose jugée, portant condamnation en raison de l'une de ces infractions ou de l'une des infractions visées à l'article 314bis, §§ 1er à 3.	§ 4. Les peines prévues aux §§ 1er à 3 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans à compter du prononcé d'un jugement ou d'un arrêt, passés en force de chose jugée, portant condamnation en raison de l'une de ces infractions ou de l'une des infractions visées à l'article 314bis, §§ 1er à 3.
§ 5. Les dispositions du § 1er, 1° et 2°, ne s'appliquent pas à la recherche la captation, l'écoute, la prise de connaissance ou l'enregistrement, par le Service Général du Renseignement et de la Sécurité des Forces armées de toute forme de communications émises à l'étranger tant à des fins militaires dans le cadre des missions explicitées à l'article 11, § 2, 1° et 2° de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité que pour des motifs de sécurité et de protection de nos troupes et de celles de nos alliés lors de missions à l'étranger et de nos ressortissants établis à l'étranger, comme explicité au même article 11, § 2, 3° et 4°.	§ 5. Les dispositions du § 1er, 1° et 2°, ne s'appliquent pas à la recherche la captation, l'écoute, la prise de connaissance ou l'enregistrement, par le Service Général du Renseignement et de la Sécurité des Forces armées de toute forme de communications émises à l'étranger tant à des fins militaires dans le cadre des missions explicitées à l'article 11, § 2, 1° et 2° de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité que pour des motifs de sécurité et de protection de nos troupes et de celles de nos alliés lors de missions à l'étranger et de nos ressortissants établis à l'étranger, comme explicité au même article 11, § 2, 3° et 4°.
LIVRE 2, TITRE V, CHAPITRE VIIIBIS – INFRACTIONS RELATIVES AU SECRET DES COMMUNICATIONS ET DES TELECOMMUNICATIONS PRIVEES.	**LIVRE 2, TITRE V, CHAPITRE VIIIBIS – INFRACTIONS RELATIVES AU SECRET DES COMMUNICATIONS NON ACCESSIBLES AU PUBLIC ET DES DONNEES D'UN SYSTEME**

	INFORMATIQUE
Article 341bis	**Article 341bis**
§ 1. Sera puni d'un emprisonnement de six mois à un an et d'une amende de deux cents euros à dix mille euros ou d'une de ces peines seulement, quiconque :	§ 1er. Sera puni d'un emprisonnement de six mois à un an et d'une amende de deux cents [euros] à dix mille [euros] ou d'une de ces peines seulement, quiconque :
1° soit, intentionnellement, à l'aide d'un appareil quelconque, écoute ou fait écouter, prend connaissance ou fait prendre connaissance, enregistre ou fait enregistrer, pendant leur transmission, des communications ou des télécommunications privées, auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications ou télécommunications;	1° soit, intentionnellement, à l'aide d'un appareil quelconque, **intercepte ou fait intercepter**, prend connaissance ou fait prendre connaissance, enregistre ou fait enregistrer des **communications non accessibles au public**, auxquelles il ne prend pas part, sans le consentement de tous les participants à ces **communications** ;
2° soit, avec l'intention de commettre une des infractions mentionnées ci-dessus, installe ou fait installer un appareil quelconque.	2° soit, avec l'intention de commettre une des infractions mentionnées ci-dessus, installe ou fait installer un appareil quelconque.
§ 2. Sera puni d'un emprisonnement de six mois à deux ans et d'une amende de cinq cents [euros] à vingt mille [euros] ou d'une de ces peines seulement, quiconque détient, révèle ou divulgue sciemment à une autre personne le contenu de communications ou de télécommunications privées, illégalement écoutées ou enregistrées, ou dont il a pris connaissance illégalement, ou utilise sciemment d'une manière quelconque une information obtenue de cette façon.	§ 2. Sera puni d'un emprisonnement de six mois à deux ans et d'une amende de cinq cents [euros] à vingt mille [euros] ou d'une de ces peines seulement, quiconque détient, révèle ou divulgue sciemment à une autre personne **le contenu de communications non accessibles au public et de données d'un système informatique illégalement interceptées ou enregistrées**, ou dont il a pris connaissance illégalement, ou utilise sciemment d'une manière quelconque une information obtenue de cette façon.
Sera puni des mêmes peines quiconque, avec une intention frauduleuse ou à dessein de nuire, utilise un enregistrement, légalement effectué, de communications ou de télécommunications privées.	Sera puni des mêmes peines quiconque, avec une intention frauduleuse ou à dessein de nuire, utilise **un enregistrement, légalement effectué, de communications non accessibles au public ou de données d'un système informatique.**
§ 2bis. Sera puni d'un emprisonnement de six mois à un an et d'une amende de deux cents euros à dix mille euros ou d'une de ces peines seulement, celui qui, indûment, possède, produit, vend obtient en vue de son utilisation, importe, diffuse ou met à disposition sous une autre forme un dispositif, y compris des données informatiques, principalement conçu ou adapté pour permettre la commission de	§ 2bis. Sera puni d'un emprisonnement de six mois à un an et d'une amende de deux cents euros à dix mille euros ou d'une de ces peines seulement, celui qui, indûment, possède, produit, vend obtient en vue de son utilisation, importe, diffuse ou met à disposition sous une autre forme un dispositif, y compris des données informatiques, principalement conçu ou adapté pour permettre la commission de

l'infraction prévue au § 1er. § 3. La tentative de commettre une des infractions visées aux §§ 1er, 2 ou 2bi est punie comme l'infraction elle-même. § 4. Les peines prévues aux §§ 1er à 3 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans à compter du prononcé d'un jugement ou d'un arrêt, passés en force de chose jugée, portant condamnation en raison de l'une de ces infractions ou de l'une des infractions visées à l'article 259bis, §§ 1er à 3.	l'infraction prévue au § 1er. § 3. La tentative de commettre une des infractions visées aux §§ 1er et 2 est punie comme l'infraction elle-même. § 4. Les peines prévues aux §§ 1er à 3 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans à compter du prononcé d'un jugement ou d'un arrêt, passés en force de chose jugée, portant condamnation en raison de l'une de ces infractions ou de l'une des infractions visées à l'article 259bis, §§ 1er à 3.
	BANQUE DE DONNEES DES EMPREINTES VOCALES
	Article 33
	Les données techniques permettant la reconnaissance vocale des personnes, faisant ou ayant fait l'objet d'une mesure d'interception des télécommunications visée à l'article 90ter, §1 du Code d'instruction criminelle et qui sont visées à l'article 44/5, §3, 1° de la loi de 5 août 1992 sur la fonction de police, sont conservées pendant 10 ans au maximum dans la Banque de données Nationale Générale visée dans la même loi, en vue d'aider à identifier ces personnes dans le cadre de dossiers d'écoute réalisés à la demande des autorités judiciaires. **Outre ces données techniques, cette banque de données contient également les données relatives au numéro de dossier, au magistrat compétent et à l'arrondissement judiciaire visé.** **Les données techniques visées au premier alinéa sont distinctes des enregistrements réalisés dans le cadre de la mise en œuvre de la mesure visée à l'article 90ter, §1 du Code d'instruction criminelle. Ces enregistrements ne sont pas concernés par le présent article.** **Les finalités et les modalités de traitement de ces données sont celles prévues aux articles 44/7 à 44/11/1 de la loi de 5 août 1992 sur la fonction de police.**