



RAAD VAN STATE
afdeling Wetgeving

CONSEIL D'ÉTAT
section de législation

advies 59.199/3
van 9 mei 2016

avis 59.199/3
du 9 mai 2016

over

sur

een voorontwerp van wet
'betreffende de verbetering van
de bijzondere
opsporingsmethoden en
bepaalde onderzoeksmethoden
met betrekking tot internet en
elektronische en
telecommunicaties'

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'

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 telecomcommunicaties’.

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.

*

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 VANNESTE, auditeur.

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 SMETS, conseiller d'État.

L'avis, dont le texte suit, a été donné le 9 mai 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.

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 politie³ 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 arbeidsauditeur⁴ 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;

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.

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.

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 39bis 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 (39ter en 39quater) 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 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 inijkoperatie 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 inijkoperatie 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 47sexies 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.

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.

2.8. Artikel 90ter 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 90quater, 90quinquies, 90sexies en 90septies 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 90ter 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 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.

⁶ Zulks klemmt 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.

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 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

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).

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 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 assistance”.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 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

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>.

¹² Over de wet van 28 november 2000, zie o.m.: 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.

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.

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.

¹³ Over de huidige wettelijke regeling inzake cybercrime, zie: J. KERKHOFS en P. VAN LINTHOUT, *Cybercrime*, Brussel, Politeia, 2013.

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 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.

¹⁴ Parl.St. Kamer, nrs. 50-0213/001 en 50-0214/001, 23-26.

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 – Transborder 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

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. These persons may retrieve the data and, provided that they have the lawful authority, they may

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.

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 88ter 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 39bis, § 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 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

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).

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*.

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 Mens²¹ en het Grondwettelijk Hof²² 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 belangen²⁴ 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 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).

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 tot 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.

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

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:

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.

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.

“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 bevindt²⁷.

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 voormelde Aanbeveling nr. R(95)13 verzocht dit verstrekken van inlichtingen te regelen met oog voor de noden van het onderzoek²⁸.

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

²⁷ Voetnoot 1 op blz. 52 van het geciteerde advies: Zie blz. 34 van het rapport bij Aanbeveling nr. R (95).

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 bedoeld op alle systemen voor de opslag, verwerking of overdracht van data. Hierbij wordt vooral

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 verschaft 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 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 beter 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*.”

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.

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 39bis, § 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 39bis, § 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 39bis, § 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:

“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’.”

Het blijft evenwel de vraag of het niet-heimelijke karakter van de zoeking niet beter in de tekst van het ontworpen artikel 39bis, § 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 39bis, § 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 39bis, § 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 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.”

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 te nemen. Dit zou dan beter 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 beter 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

³² Zie C. CONINGS, *l.c.*, 623-624.

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 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:

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.

“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 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 eenieder 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.

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.

b) de zoëven gemaakte opmerking a), klemmt 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

‘... 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 waarvan³⁷ 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

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.

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

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*quinqüies* 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*quinqüies* 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.

³⁹ GwH 21 december 2004, nr. 202/2004, B.4.2.

⁴⁰ Een gelijkaardige bepaling komt nu reeds voor in artikel 47*quinqüies*, § 3, tweede lid, van het Wetboek van Strafvordering.

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 beter 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 beter 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 geneesheren tot geheimhouding verplicht wanneer zij op de hoogte worden gebracht van de in artikel 56*bis*,

⁴¹ *L.c.*, 146-150.

derde lid, genomen maatregelen en wordt de miskennen 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*quiquies*, § 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 90*ter*, § 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 90*ter*, § 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 88*bis*, § 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 gevisieerd 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).

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 verschaft 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.

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.

1. En application de l'article 84, § 3, alinéa 1^{er}, des lois sur le Conseil d'État, coordonnées le 12 janvier 1973, la section de législation a fait porter 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.

2.1. L'article 39bis 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 88ter 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 39bis, § 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.

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.

³ En application de l'article 56, § 1^{er}, 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.

L'avant-projet prévoit également des mesures d'accompagnement en vue de permettre la mise en œuvre des mesures visées à l'article 39bis 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 (39ter et 39quater) 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 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'emporter 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 47sexies 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 90ter 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

⁵ Convention sur la cybercriminalité, faite à Budapest le 23 novembre 2001, à laquelle la loi du 3 août 2012 a donné assentiment.

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 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, § 1^{er}, alinéa 1^{er}, 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 « cyberspace » (le monde virtuel des ordinateurs) sont généralement désignées par le terme « cybercriminalité » (*cybercrime*).

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.

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 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 localisé⁷. 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 État⁸.

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 telles données⁹. La

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. 1^{er} décembre 2015, RAGB 2016, 485, note K. DE SCHEPPER).

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,

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'étranger¹⁰.

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 série d'innovations en la matière¹², 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 88ter 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

<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 recommandation 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>.

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.

l'internationalisation sans cesse croissante de la criminalité économique-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 apporter 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.

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'apporter 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 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 1^{er} 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
- 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

¹⁴ Doc. parl., Chambre, n^{os} 50-0213/001 et 50-0214/001, 23-26.

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 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.

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.

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>.

Depuis le 1^{er} 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 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 importante 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

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).

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.

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 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 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

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.

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.

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'.

(...)

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.

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, n°s 50-0213/001 et 50-0214/001, pp. 54-55.

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 informatique²⁷.

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 n° R(95)13, précitée, invite les États membres à organiser ce type d'information et ce dans le respect des impératifs de l'enquête²⁸.

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 1^{er}, en projet, du Code d'instruction criminelle (article 2, 2°, du projet) fait état d'un système « légalement » saisi³¹. Il est évident que toute saisie doit intervenir en conformité avec la loi, sans qu'il soit nécessaire de le préciser expressément.

²⁷ Note 1 à la page 24 de l'avis cité : Voir p. 34 du rapport accompagnant la recommandation n° R(95)13.

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 bedoeld 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.

9. À propos de l'article 39bis, § 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 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 39bis, § 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 39bis, § 3, alinéa 1^{er}, 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 39bis, § 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 39bis, § 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 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 39bis, § 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 39bis, § 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 39bis, § 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 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

machting 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 machtingen. 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 machting 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 39bis, § 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 39bis, § 2, en projet, de ce code.

16. L’article 39bis, § 4bis, 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 39bis, §§ 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 39bis, § 4bis, en projet, du Code d’instruction criminelle vise un système informatique qui, en fait, ne peut pas être saisi, alors que l’article 39bis, § 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 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 39bis, § 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 pertinente³². Cette question n'a toutefois pas pu être examinée plus en détail dans le délai imparti.

18. L'article 39bis, § 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 39ter, § 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 39quater, §§ 1^{er} 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 possibles³³.

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 39quater, § 2, alinéa 4, deuxième tiret (lire : 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.

³² Voir C. CONINGS, *l.c.*, 623-624.

³³ L'article 46bis, § 1^{er}, alinéas 2 et 4, en projet, du Code d'instruction criminelle (article 5 du projet) confère bel et bien cette délégation au Roi.

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 1^{er}, 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 1^{er}, en projet, du Code d'instruction criminelle (article 12, 3°, du projet).

Article 6

23. À l'article 46*quinquies*, § 1^{er}, alinéa 1^{er}, 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*, § 1^{er}, 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 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.

³⁴ Note 29 de l'avis cité : Ch. De Valkeneer, op. cit., p. 459.

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'Etat 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

'... 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}, § 1^{er}, 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,

³⁵ Note 30 de l'avis cité : Voir l'exposé des motifs, p. 18.

³⁶ Avis C.E. 32.673/2, *l.c.*, 140-142. Voir toutefois l'observation préalable de cet avis.

« [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 47octies, § 2, dernier alinéa, du Code d'instruction criminelle).

26. L'article 46sexies, § 1^{er}, alinéa 1^{er}, 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 lesquelles³⁷ 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 ministre³⁸, 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'information³⁹.

27. Les auteurs du projet vérifieront s'il n'est pas possible de préciser la notion de « circonstances exceptionnelles » figurant à l'article 46sexies, § 1^{er}, alinéa 1^{er}, 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 46sexies, § 3, envisagé du Code d'instruction criminelle ne se limitent pas nécessairement aux infractions commises dans le cyberspace.

Le rapport entre cette disposition et les articles 47quinquies et 47octies du Code d'instruction criminelle devra donc être clarifié.

29. Aux termes de l'article 46sexies, § 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 46sexies, § 1^{er}, 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 46sexies, § 3, alinéa 7, en projet, quelles infractions peuvent être commises⁴⁰. Cependant, l'article 46sexies, § 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.

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.

⁴⁰ Une disposition analogue figure déjà à l'article 47quinquies, § 3, alinéa 2, du Code d'instruction criminelle.

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. 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.

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 46sexies, § 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 56bis 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 V⁴¹.

32. Aux termes de la phrase à ajouter à l'article 56bis, alinéa 4, du Code d'instruction criminelle, le bâtonnier ou le représentant de l'ordre provincial des médecins est tenu au secret lorsqu'il est informé des mesures prises à l'article 56bis, 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 28quinquies, § 1^{er}, alinéa 2, et 57, § 1^{er}, 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^o, du projet.

Article 12

33. Au sujet de l'article 88bis, § 1^{er}, 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 ».

⁴¹ L.c., 146-150.

Article 14

34. L'article 14, 1^o, du projet a entre autres pour objet de remplacer les mots « aux personnes » par les mots « à quiconque » à l'article 88^{quater}, § 1^{er}, 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 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 gevisieerd 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).

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 ».

Il est recommandé d'insérer cette précision dans l'exposé des motifs.

Article 17

35. À l'article 90^{ter}, § 2, 36^o, en projet, du Code d'instruction criminelle (article 17, 2^o, 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 90octies, § 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.

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.

DE GRIFFIER - LE GREFFIER

DE VOORZITTER - LE PRÉSIDENT

Annemie GOOSSENS

Jo BAERT