DOC 56 **0791/001**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

17 maart 2025

WETSVOORSTEL

tot wijziging van de wet van 5 augustus 1992 op het politieambt en van het Wetboek van Strafvordering, betreffende verstorende politionele onderzoekstechnieken in een onlineomgeving en de uitbreiding van de digitale recherche

(ingediend door mevrouw Sophie De Wit c.s.)

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

17 mars 2025

PROPOSITION DE LOI

modifiant la loi du 5 août 1992 sur la fonction de police et le Code d'instruction criminelle en ce qui concerne l'utilisation de techniques d'enquête policières disruptives en ligne et l'extension de la recherche numérique

(déposée par Mme Sophie De Wit et consorts)

SAMENVATTING

Voor de aanpak van de cybercriminaliteit bepleit dit wetsvoorstel een verschuiving van louter repressieve maartregelen naar innovatieve en disruptieve methoden. De huidige reactieve aanpak van cybercriminaliteit is immers ineffectief en kost veel capaciteit en de grenzeloze aard van cybercriminaliteit bemoeilijkt de traditionele dadervervolging.

Er is evenwel een gebrek aan een wettelijk kader in België om deze innovatieve en disruptieve technieken in te zetten. Dit voorstel beoogt dan ook een aantal wetswijzigingen die nodig zijn om politiediensten in staat te stellen cybercriminaliteit te voorkomen en desgevallend effectief te vervolgen.

RÉSUMÉ

Pour lutter contre la cybercriminalité, cette proposition de loi préconise de donner la priorité à des méthodes innovantes et disruptives plutôt qu'aux méthodes purement répressives. En effet, la gestion réactive actuelle de la cybercriminalité est inefficace et nécessite beaucoup de ressources. De plus, la poursuite des cybercriminels selon la procédure traditionnelle est compliquée par le fait que la cybercriminalité ignore les frontières.

La Belgique ne s'est cependant pas encore dotée d'un cadre légal qui permette d'appliquer lesdites méthodes innovantes et disruptives. Cette proposition de loi prévoit dès lors des modifications législatives nécessaires pour permettre aux services de police d'ainsi prévenir la cybercriminalité et, le cas échéant, de poursuivre effectivement les cybercriminels.

N-VA	:	*Nieuw-Vlaamse Alliantie*
VB	:	*Vlaams Belang*
MR	:	*Mouvement Réformateur*
PS	:	*Parti Socialiste*
PVDA-PTB	:	*Partij van de Arbeid van België – Parti du Travail de Belgique*
Les Engagés	:	*Les Engagés*
Vooruit	:	*Vooruit*
cd&v	:	*Christen-Democratisch en Vlaams*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
Open Vld	:	*Open Vlaamse liberalen en democraten*
DéFI	:	*Démocrate Fédéraliste Indépendant*

Afkorting bij de nummering van de publicaties:		*Abréviations dans la numérotation des publications:*	
DOC 56 0000/000	*Parlementair document van de 56e zittingsperiode + basisnummer en volgnummer*	*DOC 56 0000/000*	*Document de la 56e législature, suivi du numéro de base et numéro de suivi*
QRVA	*Schriftelijke Vragen en Antwoorden*	*QRVA*	*Questions et Réponses écrites*
CRIV	*Voorlopige versie van het Integraal Verslag*	*CRIV*	*Version provisoire du Compte Rendu Intégral*
CRABV	*Beknopt Verslag*	*CRABV*	*Compte Rendu Analytique*
CRIV	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaalde beknopt verslag van de toespraken (met de bijlagen)*	*CRIV*	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*
PLEN	*Plenum*	*PLEN*	*Séance plénière*
COM	*Commissievergadering*	*COM*	*Réunion de commission*
MOT	*Moties tot besluit van interpellaties (beigekleurig papier)*	*MOT*	*Motions déposées en conclusion d'interpellations (papier beige)*

TOELICHTING

DAMES EN HEREN,

Om de cybercriminaliteit effectief aan te pakken, volstaat het niet om een louter repressieve strategie te hanteren. Bovendien slorpt de huidige reactieve vorm van repressieve strategie enerzijds veel capaciteit op en levert het anderzijds maar weinig resultaten op. Het verhogen van de algemene kennis en bewustwording van de bevolking door middel van preventiecampagnes vormt de eerste belangrijke sleutel in deze strijd. Daarnaast vereist de complexiteit van de cybercriminaliteit ook een fundamentele herziening van het beleid: een overstap van louter repressie naar direct inzetbare innovatieve en verstorende methoden is dan ook hoogstnoodzakelijk.

De cybercriminaliteit is grenzeloos en verweven in diverse fenomenen. De traditionele dadervervolging wordt gehinderd door landsgrenzen, geavanceerde technische methoden om sporen te maskeren, snelle financiële transacties en een gebrek aan medewerking van bepaalde landen bij de vervolging en de uitlevering. Verstorende technieken bieden een nieuw perspectief en leveren direct een verstorend resultaat op, en hebben met andere woorden een directe impact op een lopend crimineel feit.

Verschillende landen beschikken reeds over dergelijke innovatieve technieken die hun vruchten lijken af te werpen. Ook de Belgische politiediensten zijn in staat om dergelijke technieken op te zetten, doch zij stoten hierbij op een te beperkt wetgevend kader.

Een voorbeeld hiervan is een AI-tool ontwikkeld door een Britse telecomprovider in samenwerking met *White Hat Hackers*. Deze tool, gebaseerd op *Large Language Model*, voert langdurige conversaties met cybercriminelen (bijvoorbeeld bij een poging tot emotiefraude), waardoor hun activiteiten worden vertraagd en slachtoffers worden beschermd. Ook de Computer Crime Unit van de Federale Gerechtelijke Politie van Antwerpen heeft intussen een tool ontwikkeld om *phishing panels* te overspoelen met fictieve slachtoffers.

Deze *flooding*-techniek maakt het voor de cybercriminelen onmogelijk om echte van fictieve slachtoffers te onderscheiden. Bovendien werden “kwetsbaarheden” in de criminele *phishing panels* ontdekt, die de politiediensten toelaten om de controle over te nemen en zowel slachtoffers als daders te identificeren. Deze laatste techniek is vandaag technisch mogelijk, maar

DÉVELOPPEMENTS

MESDAMES, MESSIEURS,

Afin de lutter de manière efficace contre la cybercriminalité, il ne suffit pas d’adopter une stratégie purement répressive. En outre, la stratégie de réaction répressive actuellement employée exige non seulement beaucoup de ressources, mais elle ne produit que peu de résultats. La première arme importante pour remporter ce combat consiste à renforcer les connaissances générales de la population et à la sensibiliser par des campagnes de prévention. De plus, compte tenu de la complexité de la cybercriminalité, il convient de procéder à une révision fondamentale de la stratégie: il est crucial de passer d’une approche purement répressive à des méthodes innovantes et disruptives, pouvant être déployées directement.

La cybercriminalité n’a pas de frontières et se mêle à différents phénomènes. La méthode traditionnelle de poursuite des auteurs est entravée par les frontières nationales, par les techniques sophistiquées visant à effacer les traces, par la rapidité des transactions financières et par le manque de coopération de certains pays en matière de poursuite et d’extradition. La mise en œuvre de techniques disruptives offre une nouvelle approche et produit des résultats immédiats et disruptifs qui auront des conséquences directes sur les faits criminels non résolus.

Plusieurs pays disposent déjà de ces techniques innovantes, qui semblent porter leurs fruits. Les services de police belges sont également en mesure de mettre en place ces techniques, mais ils se heurtent à un cadre législatif trop restrictif.

On peut citer parmi ces techniques un outil d’intelligence artificielle développé par un fournisseur de télécommunications britannique en collaboration avec des hackers éthiques (*White Hat Hackers*). Cet outil, basé sur un grand modèle de langage (*Large Language Model*), mène de longues conversations avec les cybercriminels (par exemple, en cas de tentative de fraude à l’émotion), ce qui permet de ralentir leurs activités et de protéger les victimes. La Computer Crime Unit de la Police judiciaire fédérale d’Anvers a également développé un outil visant à submerger les *phishing panels* de victimes fictives.

Cette technique d’inondation (*flooding*) empêche les cybercriminels de distinguer les véritables victimes des victimes fictives. En outre, des “vulnérabilités” ont été découvertes au niveau des *phishing panels*. Les services de police peuvent dès lors en prendre le contrôle et identifier tant les victimes que les auteurs. Bien que la technologie nécessaire soit déjà disponible en la

mist een voldoende wettelijke basis om onmiddellijk te kunnen worden ingezet. Een wetswijziging dringt zich dan ook op om de politiediensten in staat te stellen om slachtoffers van cybercriminaliteit in de eerste plaats te voorkomen en cybercriminelen vervolgens ook effectief te vervolgen.

TOELICHTING BIJ DE ARTIKELEN

Artikel 2

Hoewel het Hof van Cassatie bij arrest van 28 maart 2017[1] heeft bevestigd dat artikel 26 van de wet van 5 augustus 1992 op het politieambt – in combinatie met artikel 8 van het Wetboek van Strafvordering – politiediensten toelaat om publiek toegankelijke plaatsen op het internet te betreden om onder meer opdrachten van gerechtelijke politie uit te voeren, is het toch aangewezen dat dit ook effectief wettelijk wordt verankerd. Op die manier is het ook mogelijk om in een onlineomgeving de opdrachten van zowel de bestuurlijke als de gerechtelijke politie uit te voeren.

De beoogde "disruptieve technieken" kunnen worden opgesplitst in twee fases, al naargelang de finaliteit. In een eerste fase wordt beoogd om slachtoffers te voorkomen, en dus (nog) niet om bewijzen te verzamelen of daders te vatten (cf. art. 15 van wet van 5 augustus 1992 op het politieambt). De technieken verwijzen in deze naar de mogelijkheid om de opdrachten van bestuurlijke politie ook in een onlineomgeving uit te voeren, zoals het "onlinepatrouilleren", het terugdringen van criminele phishing panels door deze te overspoelen met fictieve slachtoffers (zonder dat het hier gaat om fictieve identiteiten), en het terugdringen van websites van cryptofraude door daar eveneens valse informatie op af te sturen dan wel een grote hoeveelheid aan nutteloze data opdat de criminele website zou platvallen.

Zelfs gerichte verificaties en communicaties met het oog op een arrestatie, weliswaar zonder het aannemen van een geloofwaardige fictieve identiteit, zijn mogelijk zonder de verplichting om een infiltratieprocedure op te starten. Deze uitzondering werd expliciet in artikel 46*sexies* van het Wetboek van Strafvordering opgenomen om niet te raken aan het autonoom politieoptreden onder

[1] *https://www.stradalex.com/nl/sl_src_publ_jur_be/document/cass_N-20.170.328-7*

matière, il n'existe pas encore aujourd'hui de base légale suffisante pour pouvoir recourir immédiatement à cette méthode. Il s'impose dès lors de modifier la législation dans les plus brefs délais pour permettre aux services de police, dans un premier temps, d'empêcher que des personnes soient victimes d'actes de cybercriminalité et, dans un deuxième temps, de poursuivre effectivement les cybercriminels.

COMMENTAIRE DES ARTICLES

Article 2

Bien que la Cour de cassation ait confirmé, dans son arrêt du 28 mars 2017[1] que l'article 26 de la loi du 5 août 1992 sur la fonction de police, combiné à l'article 8 du Code d'instruction criminelle, autorise les services de police à accéder aux lieux de connexion à internet, considérés comme publics, notamment dans le but de mener à bien les missions de police judiciaire, il s'indique d'inscrire ces dispositions dans la loi de manière effective. Les missions de police administrative et judiciaire pourront ainsi aussi s'exercer en ligne.

Les "techniques disruptives" envisagées peuvent se répartir en deux phases, selon leur finalité. L'objectif de la première phase est d'éviter des victimes, et donc pas (encore) de rassembler des preuves ou d'arrêter des auteurs (*cf.* art. 15 de la loi du 5 août 1992 sur la fonction de police). Ces techniques renvoient en l'espèce à la possibilité d'accomplir les missions de police administrative en ligne également, en "patrouillant sur internet", le démantèlement, les réseaux criminels spécialisés dans l'hameçonnage, en les inondant de fausses victimes (sans qu'il s'agisse d'identités fictives), et le démantèlement de sites frauduleux liés aux cryptomonnaies en leur envoyant aussi des informations erronées ou une grande quantité de données inutiles, de manière à les faire planter.

Il est même possible de procéder à des vérifications et à des communications ciblées en vue d'une arrestation sans devoir entamer une procédure d'infiltration, mais alors sans prendre une identité fictive crédible. Cette exception a été explicitement inscrite à l'article 46*sexies* du Code d'instruction criminelle pour ne pas porter atteinte à l'autonomie d'intervention des fonctionnaires

[1] *https://www.stradalex.com/fr/sl_src_publ_jur_be/document/cass_F-20.170.328-7*

artikel 26 van de wet op het politieambt.[2] Aangezien het al dan niet gebruikmaken van een geloofwaardige fictieve identiteit niet altijd even duidelijk uit te maken is, lijkt een verduidelijking in het Wetboek van Strafvordering en in de wet op het politieambt hieromtrent wel aangewezen.

Het komt erop neer dat er geen duurzame vorm van contact tussen agent en verdachte mag plaatsvinden tijdens een autonoom optreden onder artikel 26 van de wet op het politieambt. Is dit wel het geval, dan zijn de specifieke regels van de internetinfiltratie (artikel 46*sexies* Wetboek van Strafvordering) immers van toepassing. Echter, in deze eerste fase waar het voorkomen van slachtoffers het primaire doel is, is er in de regel geen duurzaam contact tussen agent en verdachte, zodat wel degelijk een beroep kan worden gedaan op voormeld artikel 26.

Artikelen 3 en 4

Indien deze politionele technieken in een digitale omgeving toch als te verregaand worden beschouwd – en hoe dan ook voor die technieken die zonder meer verdergaan – moeten tevens enkele artikelen in het Wetboek van Strafvordering worden gewijzigd, met name artikel 28*bis* (proactieve recherche)[3] en artikel 46*sexies* (online-infiltratie).

In het ontworpen derde lid van de eerste paragraaf van artikel 46*sexies* van het Wetboek van Strafvordering (artikel 4 van het wetsvoorstel) wordt bepaald dat de Koning bij een besluit vastgesteld na overleg in de Ministerraad, op voordracht van de minister van Justitie en na advies van het College van procureurs-generaal, de virtuele politionele onderzoekstechnieken dient te bepalen. Deze onderzoekstechnieken blijven daarbij niet beperkt tot

[2] Artikel 46*sexies*, § 1, laatste lid van het Wetboek van Strafvordering luidt als volgt: “Dit artikel is niet van toepassing op de persoonlijke interactie op het internet van politieambtenaren, bij de uitvoering van hun opdrachten van gerechtelijke politie, met een of meerdere personen, die enkel een gerichte verificatie of een arrestatie tot direct doel heeft, en dit zonder gebruik te maken van een geloofwaardige fictieve identiteit.”

[3] Onder “proactieve recherche” wordt verstaan: het opsporen, het verzamelen, registreren en verwerken van gegevens en inlichtingen op grond van een redelijk vermoeden van te plegen of reeds gepleegde maar nog niet aan het licht gebrachte strafbare feiten, met het doel te komen tot het vervolgen van daders van misdrijven, en die worden of zouden worden gepleegd in het kader van een criminele organisatie, zoals gedefinieerd door de wet, of misdaden of wanbedrijven als bedoeld in artikel 90*ter,* §§ 2, 3 en 4, uitmaken of zouden uitmaken. Het instellen van een proactieve recherche behoeft voorafgaande schriftelijke toestemming, door de procureur des Konings, de arbeidsauditeur, (of de federale procureur) gegeven in het kader van hun respectieve bevoegdheid, onverminderd de naleving van de specifieke wettelijke bepalingen die de (bijzondere opsporingsmethoden en andere methoden) regelen.

de police prévue à l’article 26 de la loi sur la fonction de police.[2] Dès lors qu’il n’est pas toujours aisé de déterminer si une identité fictive crédible a été utilisée ou pas, il semble indiqué d’apporter des précisions à ce sujet dans le Code d’instruction criminelle et dans la loi sur la fonction de police.

Il est prévu, en substance, qu’il ne pourra pas y avoir de contacts prolongés entre l’agent et le suspect au cours d’une intervention autonome menée en application de l’article 26 de la loi sur la fonction de police. En cas de contacts prolongés, les règles spécifiques encadrant l’infiltration sur Internet (article 46*sexies* du Code d’instruction criminelle) seront en effet d’application. À l’inverse, au cours de cette première phase, dont l’objectif premier sera d’éviter des victimes, tout contact prolongé entre l’agent et le suspect sera exclu, en principe, si bien que l’article 26 précité pourra effectivement s’appliquer.

Articles 3 et 4

Étant donné que ces techniques policières dans un environnement numérique peuvent néanmoins être jugées excessives – et, en tout état de cause, pour les techniques policières avancées en général –, il convient également de modifier certains articles du Code d’instruction criminelle, à savoir ses articles 28*bis* (enquête proactive)[3] et 46*sexies* (infiltration en ligne).

L’article 46*sexies*, § 1er, alinéa 3, en projet, du Code d’instruction criminelle (article 4 de la proposition de loi) prévoit que le Roi devra préciser les techniques d’enquête policières virtuelles par arrêté délibéré en Conseil des ministres, sur la proposition du ministre de la Justice et après avis du Collège des procureurs généraux. Ces techniques d’enquête ne seront en outre pas strictement limitées aux unités spéciales mais,

[2] L’article 46*sexies*, § 1er, dernier alinéa, du Code d’instruction criminelle s’énonce comme suit: “Le présent article ne s’applique pas à l’interaction personnelle de fonctionnaires de police, dans l’exercice de leurs missions de police judiciaire, avec une ou plusieurs personnes sur Internet, qui n’a pour finalité directe qu’une vérification ciblée ou une arrestation, et ceci sans utiliser d’identité fictive crédible.”

[3] Par “enquête proactive”, on entend, dans le but de permettre la poursuite d'auteurs d'infractions, la recherche, la collecte, l'enregistrement et le traitement de données et d'informations sur la base d'une suspicion raisonnable que des faits punissables vont être commis ou ont été commis mais ne sont pas encore connus, et qui sont ou seraient commis dans le cadre d'une organisation criminelle, telle que définie par la loi, ou constituent ou constitueraient un crime ou un délit tel que visé à l'article 90*ter*, §§ 2, 3 et 4. Pour entamer une enquête proactive, l'autorisation écrite et préalable du procureur du Roi, de l'auditeur du travail, ou du procureur fédéral, dans le cadre de leur compétence respective, est requise, sans préjudice du respect des dispositions légales spécifiques réglant les méthodes particulières de recherche et autres méthodes.

de bijzondere eenheden maar worden, teneinde zekere waarborgen in te bouwen, wel voorbehouden voor de gespecialiseerde afdelingen van de gerechtelijke politie, eventueel gekoppeld aan bepaalde profielen of het slagen in bepaalde bijkomende opleidingen (zoals dat nu al is voorzien voor de virtuele infiltratie).

Daarbij is het zowel bij de proactieve recherche als bij de online-infiltratie van belang dat aan de volgende criteria is voldaan:

1) machtiging door de procureur des Konings (zoals al voorzien in de artikelen 28*bis*, § 2, en 46*sexies*, § 2, van het Wetboek van Strafvordering);

2) het uitvoerig documenteren van de politionele actie, waarbij de voorkeur wordt gegeven aan een vertrouwelijk verslag in plaats van een proces-verbaal (zoals momenteel bepaald in artikel 46*sexies*, § 4, van het Wetboek van Strafvordering). Uiteraard wordt er wel een proces-verbaal opgesteld wanneer er al effectief slachtoffers (in België) bekend zijn;

3) een duidelijke onderbouwing van de noodzaak, proportionaliteit en subsidiariteit van de politionele actie.

In een tweede fase is het ten slotte wel degelijk de bedoeling om de daders ook effectief te vatten, waarvoor eveneens een beroep kan worden gedaan op artikel 46*sexies* van het Wetboek van Strafvordering. Om de daders te kunnen lokaliseren (teneinde de bevoegdheidsgrond te bepalen) is het in bepaalde gevallen noodzakelijk voor de politiediensten om zelf misdrijven te plegen, waaronder bijvoorbeeld hacking.

Conform artikel 46*sexies* worden zulke handelingen wettelijk omkaderd. Zodra de daders vervolgens zijn gelokaliseerd en er sprake is van een Belgische link, kan het onderzoek zijn verder verloop kennen waarbij zowel een proces-verbaal wordt opgesteld alsook een vertrouwelijk verslag waarin de informatie en het procesverloop transparant worden gedeeld.

Sophie De Wit (N-VA)
Christoph D'Haese (N-VA)
Kristien Van Vaerenbergh (N-VA)

afin de prévoir certaines garanties, leur utilisation sera néanmoins réservée aux sections spécialisées de la police judiciaire, voire à certains profils ou aux agents ayant achevé certaines formations complémentaires avec fruit (comme c'est déjà actuellement prévu pour l'infiltration virtuelle).

À cet égard, il est essentiel que l'enquête proactive, tout comme l'infiltration en ligne, remplisse les critères suivants:

1) avoir obtenu l'autorisation du procureur du Roi (comme déjà prévu aux articles 28*bis*, § 2, et 46*sexies*, § 2, du Code d'instruction criminelle);

2) documenter en détail l'action policière, de préférence sous la forme d'un rapport confidentiel plutôt que d'un procès-verbal (conformément aux dispositions actuelles de l'article 46*sexies*, § 4, du Code d'instruction criminelle). Un procès-verbal est bien sûr rédigé lorsqu'il existe déjà des victimes connues (en Belgique);

3) justifier clairement le caractère nécessaire, proportionnel et subsidiaire de l'action policière.

Dans la deuxième phase, l'objectif est d'aboutir à l'arrestation effective des auteurs, pour laquelle l'article 46*sexies* du Code d'instruction criminelle peut également être invoqué. Afin de localiser ces auteurs (et de déterminer le fondement de la compétence), les services de police doivent parfois commettre eux-mêmes des infractions, telles que le piratage informatique.

Conformément à l'article 46*sexies*, ces actes sont encadrés par la loi. Dès lors que les auteurs ont été localisés et qu'un lien avec la Belgique a été établi, l'enquête peut se poursuivre avec la rédaction d'un procès-verbal et d'un rapport confidentiel dans lequel les informations et le déroulement de l'enquête sont partagés de manière transparente.

WETSVOORSTEL

Artikel 1

Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

Art. 2

In artikel 26 van de wet van 5 augustus 1992 op het politieambt, gewijzigd bij de wet van 7 december 1998, wordt tussen het eerste en het tweede lid, dat het derde lid wordt, een lid ingevoegd, luidende:

“Voor de toepassing van deze wet worden de voor het publiek toegankelijke plaatsen op het internet of op andere elektronische communicatienetwerken, ongeacht of er voor het nemen van de toegang daartoe bepaalde vormelijke toegangsformaliteiten moeten worden ondernomen, gelijkgesteld met publiek toegankelijke plaatsen. De politieambtenaren mogen deze plaatsen bezoeken, bestuderen en er kopieën van nemen.”

Art. 3

Artikel 28*bis*, § 2*,* van het Wetboek van Strafvordering, laatstelijk gewijzigd bij de wet van 6 januari 2003, wordt aangevuld met een lid, luidende:

“De proactieve recherche strekt zich ook uit over het internet of andere elektronische communicatienetwerken.”

Art. 4

In artikel 46*sexies*, § 1, van het Wetboek van Strafvordering, ingevoegd bij de wet van 25 december 2016, wordt tussen het tweede en het derde lid, dat het vierde lid wordt, een lid toegevoegd, luidende:

“De procureur des Konings kan de politiediensten tevens machtigen om, binnen het wettelijk kader van een infiltratie en met inachtneming van de finaliteit ervan, bepaalde virtuele politionele onderzoekstechnieken aan te wenden. De Koning bepaalt bij een besluit vastgesteld na overleg in de Ministerraad,, op voordracht van

PROPOSITION DE LOI

Article 1er

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

Art. 2

Dans l’article 26 de la loi du 5 août 1992 sur la fonction de police, modifié par la loi du 7 décembre 1998, entre l’alinéa 1er et l’alinéa 2, qui devient l’alinéa 3, il est inséré un alinéa rédigé comme suit:

“Pour l’application de la présente loi, les lieux accessibles au public sur l’internet ou sur d’autres réseaux de communications électroniques, que leur accès requière ou non certaines formalités de forme, sont assimilés à des lieux accessibles au public. Les fonctionnaires de police peuvent visiter ces lieux, les étudier et en réaliser des copies.”

Art. 3

L’article 28*bis*, § 2, du Code d’instruction criminelle, modifié en dernier lieu par la loi du 6 janvier 2003, est complété par un alinéa rédigé comme suit:

“L’enquête proactive s’étend également à l’internet ou à d’autres réseaux de communications électroniques.”

Art. 4

Dans l’article 46*sexies*, § 1er, du Code d’instruction criminelle, inséré par la loi du 25 décembre 2016, un alinéa rédigé comme suit est inséré entre les alinéas 2 et 3:

“Le procureur du Roi peut également autoriser les services de police à recourir à certaines techniques d’enquête policières virtuelles, dans le cadre légal d’une infiltration et dans le respect de la finalité de celle-ci. Le Roi précise par un arrêté délibéré en Conseil des ministres, sur la proposition du ministre de la Justice

de minister van Justitie en na advies van het College van procureurs-generaal, deze virtuele politionele onderzoekstechnieken."

13 februari 2025

Sophie De Wit (N-VA)
Christoph D'Haese (N-VA)
Kristien Van Vaerenbergh (N-VA)

et après avis du Collège des procureurs généraux, ces techniques d'enquête policières virtuelles.".

13 février 2025

Centrale drukkerij - Imprimerie centrale