UCL Université catholique de Louvain

Faculté de droit et de criminologie (DRT)

Nos instruments pénaux, sont-ils efficaces pour lutter contre les infractions de criminalité informatique ?

Analyse et commentaire du droit pénal matériel et procédural belge

Mémoire réalisé par
Caroline HEYMANS

Promoteur(s)
Marie-Aude BEERNAERT

Année académique 2014-2015
Master en droit

Plagiat et erreur méthodologique grave

Le plagiat entraîne l'application des articles 87 à 90 du règlement général des études et des examens de l'UCL.

Il y a lieu d'entendre par « plagiat », l'utilisation des idées et énonciations d'un tiers, fussent-elles paraphrasées et quelle qu'en soit l'ampleur, sans que leur source ne soit mentionnée explicitement et distinctement à l'endroit exact de l'utilisation.

La reproduction littérale du passage d'une œuvre, même non soumise à droit d'auteur, requiert que l'extrait soit placé entre guillemets et que la citation soit immédiatement suivie de la référence exacte à la source consultée.*.

En outre, la reproduction littérale de passages d'une œuvre sans les placer entre guillemets, quand bien même l'auteur et la source de cette œuvre seraient mentionnés, constitue une erreur méthodologique grave pouvant entraîner l'échec.

* A ce sujet, voy. notamment **http://www.uclouvain.be/plagiat**.

TABLE DES MATIÈRES

REMERCIEMENTS

La réalisation de ce mémoire fut possible grâce à l'aide, les encouragements et l'encadrement de plusieurs personnes auxquelles je souhaite adresser ces remerciements.

Je souhaite remercier en premier lieu ma promotrice, la Professeur Marie-Aude Beernaert, de m'avoir encadrée dès ma première année de Master en droit afin de me donner tous les outils nécessaires à la réalisation de ce mémoire. Je la remercie pour sa disponibilité, ses conseils judicieux, ses encouragements et sa patience.

Je remercie également Koen Smets, inspecteur principal au FCCU et Marjolein Delplace, analyste stratégique du FCCU de m'avoir accordé de leur temps pour me parler de leur métier et pour répondre à mes questions. Grâce à leur précieuse aide, j'ai pu acquérir une meilleure maîtrise de mon sujet.

Je souhaite enfin exprimer ma reconnaissance envers ma famille pour leur soutien durant l'ensemble de mes études et plus particulièrement durant la rédaction de mon mémoire.

LEXIQUE INFORMATIQUE ET ABRÉVIATIONS

Adresse IP	Un numéro d'identification appartenant à chaque appareil connecté à un réseau informatique
Advanced Persistant Threat	Les APT sont des attaques mettant en œuvre diverses techniques et ayant pour but d'attaquer un système informatique sur la durée, sans être repérées. Il s'agit d'attaques difficilement visibles mais à impacts énormes.
Cloud	Le cloud ou *cloud computing* est une infrastructure permettant de partager des données avec tout utilisateur qui en fait la demande via un simple portail internet. L'usage le plus fréquent du cloud est de stocker des données sur un « nuage » en ligne ce qui permet ensuite de les consulter depuis n'importe quel ordinateur, via internet.
Crypter	Coder un message qui rend celui-ci illisible pour ceux qui ne disposent pas de la clé de cryptage.
Crypto-ransomware	Une forme de *malware* qui crypte les données d'un ordinateur et les rend illisibles pour son propriétaire tant qu'une somme d'argent n'a pas été payée.
Dark-web	Le *dark-web* fait référence aux sites internet qui ne sont pas trouvables via les moteurs de recherches traditionnels. L'accès à ces sites se fait généralement par le réseau TOR qui assure un anonymat. Le *dark web* est utilisé principalement pour la commission d'infractions.
Data	Données informatiques
Defacement	Modification indésirable de la présentation d'un site web.
E-banking	Les services bancaires électroniques
E-Cops	Ancien point de contact de la police fédérale belge pour signaler des délits commis sur internet. Il ne s'agit pas d'un point de contact pour établir une plainte en ligne.
FCCU	*Federal Computer Crime Unit.* Section de la police fédérale, spécialisée dans la criminalité informatique.
Malware	Logiciel malveillant

NTIC	Nouvelles Techniques d'Information et de Communication.
Numéro IMEI	Numéro d'identification d'un téléphone mobile.
Phishing	Hameçonnage. Technique utilisée par les délinquants pour rentrer en possession de données personnelles de leurs victimes.
Police Ransomware	Un *malware* bloquant l'accès à un ordinateur, soi-disant au nom de la police, et requérant le payement d'une « amende » afin de récupérer l'accès, par le propriétaire de l'ordinateur, à ses données.
Ransomware	Un *malware* infectant les ordinateurs tant qu'une somme d'argent n'est pas payée.
RCCU	*Regional Computer Crime Unit.* Une section de la police au niveau de chaque arrondissement judiciaire qui est spécialisée en criminalité informatique.
Serveur	Un serveur est un ordinateur qui s'utilise pour l'administration d'un réseau informatique. Le serveur gère l'accès aux ressources et aux différents périphériques ainsi que les connexions des utilisateurs.
The Onion Router (TOR)	Un logiciel légal permettant de surfer sur les réseaux en tout anonymat. Ce logiciel est principalement utilisé pour accéder au *dark-web* et pour la commission d'infractions en tout anonymat.

« *La révolution informatique a fourni les outils permettant de voler en toute impunité, de contrôler et de manipuler les pensées et les mouvements de millions de gens et de tenir une société entière en otage. D'un autre coté s'il est bien employé, l'ordinateur peut améliorer de façon notable la vie de milliards d'habitants de la planète. Le choix est dans nos mains. L'avenir de l'humanité ne doit pas obligatoirement être un avenir de criminalité informatique et de terreur* »[1]

- August BEQUAI
Washington DC, avril 1990

[1] Préface de la Recommandation n° R (89) 9 sur la criminalité en relation avec l'ordinateur du 9 septembre 1989, adoptée le 13 septembre 1989, Editions du Conseil de l'Europe, Strasbourg, 1990, disponible sur http://www.coe.fr/cm/ta/rec/1989/f89r9.htm.

INTRODUCTION

Aujourd'hui, 83% des ménages belges disposent d'une connexion internet[2]. Au niveau de la moyenne européenne pas moins de 81% des personnes utilisent de façon régulière cet outil[3]. Et dans certains pays voisins, on atteint plus de 90%[4]. Ces hauts pourcentages n'ont cessé de croître ces dernières années[5] et tout porte à croire que cette tendance continuera.

Les nouvelles technologies d'information et de communication nous apportent une quantité infinie de nouvelles possibilités, ce qui facilite notre vie au quotidien. Les avantages liés aux NTIC[6] expliquent leur omniprésence dans notre société.

Toutefois, ces possibilités et avantages ne s'offrent pas uniquement aux gens bien intentionnés. Les délinquants se servent également de plus en plus des nouvelles technologies pour la commission de leurs délits traditionnels. De plus, l'existence-même de ces nouvelles technologies mène à la création de nouveaux types de délits, propres au cybermonde. L'ensemble de ces délits commis dans le monde informatique est ce qui est actuellement entendu sous le vocable « cybercriminalité ».

Alors qu'en 2014 la criminalité traditionnelle est en baisse, la cybercriminalité ne cesse de croître[7]. Une étude récente estime que chaque minute trois belges sont victimes de criminalité informatique[8]. Ces chiffres sont inquiétants…

Au vu de l'importance de ce phénomène, nous avons choisi d'aborder, dans le cadre de ce mémoire, la situation de la cybercriminalité, principalement en Belgique, afin de poser un regard critique sur l'encadrement juridique tant d'un point de vue du droit pénal matériel que procédural.

---

[2] Voy. l'annexe n° 6 afin de trouver le tableau complet des statistiques de StatBel, la direction statistique du SPF Économie, à propos de l'utilisation d'Internet auprès des ménages belges.
[3] Voy. l'annexe n° 7 afin de trouver le tableau complet des statistiques de EuroStat, la direction statistique de la Commission européenne, à propos de l'utilisation d'Internet auprès des ménages européens.
[4] Voy. l'annexe n° 7 afin de trouver le tableau complet des statistiques de EuroStat, la direction statistique de la Commission européenne, à propos de l'utilisation d'Internet auprès des ménages européens.
[5] Voy. l'annexe n° 9 afin de trouver le tableau complet des statistiques du ministère public sur le flux d'entrée des affaires de type « informatique » de 2003 à 2014.
[6] Lorsque l'acronyme NTIC sera utilisé dans ce mémoire, il sera fait référence aux Nouvelles Technologies d'Information et de Communication.
[7] T. DEPLA, « Politie registreerde 3,7% minder criminele feiten in 2014 », 15 juillet 2015, disponible sur: http://www.polinfo.be.
[8] En effet, le *Norton Cybercrime Report* de l'année 2011 évalue que 1,4 million de Belges furent victimes de cybercriminalité en 2010. Ceci correspond à trois belges par minutes.
Rapport de *Norton by Symantec* disponible sur : http://be.norton.com/cybercrimereport.

La première partie de ce mémoire (Partie I) dressera le tableau général afin de comprendre ce qu'est la cybercriminalité et dans quelle mesure elle impacte notre société. Les principaux concepts y seront expliqués et des statistiques interpellantes tenteront de faire prendre conscience au lecteur de l'importance qu'a acquis ce phénomène.

Dans la deuxième partie (Partie II), les différentes infractions de cybercriminalité prévues par le droit pénal matériel seront expliquées et un regard critique sera posé sur l'efficacité de ce cadre pénal et sur les points qui nécessitent une amélioration.

La troisième partie de ce mémoire (Partie III) vise, quant à elle, le droit procédural pénal du cybermonde et les principaux problèmes rencontrés par les autorités de recherche et de poursuite dans un environnement numérique. Dans cette partie un regard critique sera également posé sur l'encadrement législatif et les mécanismes de recherche et de poursuite.

L'objectif de ce mémoire est de mettre en lumière les principaux problèmes liés au cybermonde qui subsistent encore aujourd'hui en droit pénal matériel et procédural et de tenter d'y apporter des éventuelles pistes de solution. Nous espérons conscientiser les lecteurs à l'omniprésence de ce phénomène et à la nécessité de réagir rapidement pour éviter que les cyberdélinquants n'acquièrent une trop grande longueur d'avance.

PARTIE I. GÉNÉRALITÉS

Dans cette première partie, le cadre général pour la compréhension du concept de cybercriminalité sera figé. La notion de cybercriminalité sera expliquée (Chapitre I) ainsi que les effets néfastes de celle-ci et les raisons de la nécessité d'une règlementation en la matière (Chapitre II). Enfin, le cadre juridique belge sera brièvement abordé (Chapitre III).

Chapitre I. La notion de cybercriminalité

Afin de comprendre la notion de cybercriminalité, nous aborderons successivement l'émergence de la cybercriminalité en Belgique (Section I) et sur la scène internationale (Section II) ainsi que son contenu (Section III) et les différentes manières de la classifier (Section IV).

Section I. Émergence de la cybercriminalité en Belgique

La notion de cybercriminalité est une notion récente qui a émergé il y a une quinzaine d'années seulement. Son émergence est due à la prolifération des nouvelles techniques d'information et de communication et à la transformation de la société moderne en une société de l'information.

La société de l'information est une société dans laquelle les techniques d'information et de communication occupent une place centrale et où la demande de numérisation et de connectivité ne cesse d'augmenter[9]. Ce modèle sociétal s'oppose à la société industrielle et se caractérise par le fait que ses membres se relationnent entre eux par la participation à travers les NTIC[10].

La société de l'information, dans laquelle nous vivons actuellement, ne s'est pas créée en un jour. Néanmoins, son émergence fut rapide et entraîna avec elle les premiers délits informatiques.

En Belgique, durant les années soixante, on peut observer les premières formes de nouvelles techniques d'information et de communication. En effet, c'est à cette époque-là que les premières bases de données informatiques surgissent. La « police et d'autres organismes sont [déjà] en mesure de stocker et de consulter de larges volumes de données »[11]. Le stockage de

[9] Union Internationale des Télécommunications, *Comprendre la Cybercriminalité : guide pour les pays en développement*, UIT, Genève, 2009, p. 11.
[10] *Ibidem*
[11] Conseil de l'Europe, *Criminalité organisée en Europe : la menace de la cybercriminalité*, Rapport de situation 2004, Editions du Conseil de l'Europe, 2006, p. 91.

ces données entraîne les quelques premiers délits informatiques qui, pour la plupart, consistent en des violations du droit à la vie privée[12].

Ces délits informatiques sont très peu fréquents et les NTIC ne connaissent pas encore un accès généralisé. Pour cette raison, il n'y a pas de réelle préoccupation concernant la criminalité informatique en Belgique à cette époque.

Dans les années septante et quatre-vingt de nouveaux délits informatiques surgissent, tels que des infractions économiques ou des infractions à la propriété intellectuelle[13]. La principale raison de l'émergence de ces typologies de délits dans le cybermonde est le fait que l'accès à l'informatique se soit généralisé au sein de l'entreprenariat[14].

Le nombre de délits informatiques croît et fait entrer la notion de criminalité informatique dans la doctrine belge. Le législateur également se rend compte de la problématique et élabore en 1988 deux projets de lois ambitieux, qui certes, n'ont jamais abouti[15].

C'est dans le courant des années nonante, avec la création des réseaux informatiques, qu'une typologie élargie de comportements informatiques nuisibles surgit. Depuis et jusqu'au jour d'aujourd'hui, cela n'a cessé d'augmenter[16]. Les nouvelles technologies offrent de plus en plus de possibilités qui sont exploitées, entre autres, pour la commission d'une panoplie de nouveaux comportements, chaque fois plus complexes.

L'affaire *BisTel*[17] surgit au tout début des années nonante et est la première affaire belge significative en termes de criminalité informatique. Etant donné qu'aucune législation spécifique n'existe alors en la matière, des constructions farfelues sont opérées afin d'essayer de punir les infractions de criminalité informatique. Toutefois, sans succès.

Cette affaire, que nous aborderons dans les chapitres suivants, va confronter la Belgique avec le vide juridique important et l'impunité qui en découle pour les auteurs de la criminalité informatique. Ce fut une prise de conscience brutale pour la justice belge, qui prit la décision d'emboiter le pas à ses voisins et de réagir dans les plus brefs délais.

---

[12] *Ibidem*
[13] *Ibidem*
[14] *Ibidem*
[15] CH. 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, p. 620.
[16] Conseil de l'Europe, *Criminalité organisée en Europe : la menace de la cybercriminalité, op. cit.*, pp. 91 à 92.
[17] En première instance, l'affaire *BisTel* : Corr. Bruxelles, 8 novembre 1990, *J.T.*, 1990, p.11. En degré d'appel, l'affaire *BisTel* : Bruxelles, 24 juin 1991, *R.D.P.C.*, 1992, p. 340.
L'affaire *BisTel* sera analysée en détail dans les prochains chapitres.

Toutefois, les réactions du législateur belge furent relativement lentes. Alors qu'après l'affaire *BisTel* la cybercriminalité devint une réelle préoccupation, le législateur belge n'intervint qu'en novembre 2000 pour la première fois[18]. À ce moment, les notions de cybercriminalité et de criminalité informatique entrèrent enfin dans l'arsenal législatif belge.

Section II. Émergence de la cybercriminalité dans le contexte des organisations internationales

Diverses organisations internationales telles que l'O.C.D.E. (§1), le G8, (§2), les Nations Unies (§3) et le Conseil de l'Europe (§4) se sont également préoccupés de la cybercriminalité, souvent bien avant la Belgique.

§1. Émergence de la notion de cybercriminalité au sein de l'O.C.D.E.

L'organisation pour la coopération et le développement économique est une organisation qui a pour but d'améliorer le bien-être socio-économique au niveau mondial. Cette organisation fut créée en 1961 et comporte aujourd'hui 34 pays-membres, dont la Belgique[19].

L'O.C.D.E. fut la première organisation internationale à se préoccuper de la cybercriminalité[20]. Dès la fin des années quatre-vingt, un comité au sein de l'O.C.D.E se pencha sur diverses questions de cybersécurité et une recommandation établissant des lignes directrices pour la sécurité des systèmes informatiques fut élaborée en 1992[21].

Ce premier acte international avait pour but de recommander aux états d'instaurer des règles de sécurité minimales en matière de cybercriminalité. Il était dépourvu de force obligatoire mais cependant il n'était pas négligeable[22]. En effet, il fut le point de départ de l'émergence de la notion de cybercriminalité à un niveau international.

Dans les années qui suivirent, diverses rencontres eurent lieu et plusieurs rapports d'une importance signifiante furent élaborés en son sein[23]. L'O.C.D.E. continue encore à l'heure actuelle de se préoccuper de la menace grandissante de la cybercriminalité.

---

[18] Loi du 28 novembre 2000 relative à la criminalité informatique, *M.B.*, 3 février 2001, ci-après dénommée loi du 28 novembre 2000.
[19] Pour de plus amples informations sur l'O.C.D.E., voy. http://www.oecd.org/fr.
[20] I. COLLARD, « Le juriste peut-il aussi être un cybercriminel ? », *L'informatique, l'Internet et le juriste,* sous la direction de J.-F. HENROTTE, Limal, Anthémis, 2010, pp. 182 à 183.
[21] Lignes directrices de l'O.C.D.E. régissant la sécurité des systèmes et réseaux d'information – vers une culture de la sécurité, du 26 novembre 1992, C(92)188, Organisation de Coopération et de Développement Économiques.
[22] A. DEBAETS e.a., « Cybercriminaliteit », *Aspecten van Europees materieel strafrecht,* sous la direction de G. VERMEULEN, Anvers, Apeldoorn-Maklu, 2002, pp. 392 à 394.
[23] *Ibidem*

§2. Émergence de la notion de cybercriminalité au sein du G8

Le G8 est un groupe intergouvernemental formé de huit grandes puissances mondiales sur le plan économique[24]. Ce groupe se réunit une fois par an afin de discuter de problématiques à caractère économique, financier ou politique.

En raison des pertes financières qu'elle engendre, la cybercriminalité fut abordée lors de ces réunions dès les années nonante et un sous-groupe spécifique pour les *high-tech crimes* fut créé au sein du G8 dès 1996[25]. Le problème fut abordé sérieusement dès le départ.

L'approche de la cybercriminalité adoptée par le G8 est importante, principalement en raison de son plan d'action comportant dix points qui établit des lignes directrices pour une lutte effective en la matière[26].

A quasi chaque sommet du G8, la criminalité informatique reste un des sujets abordés G8[27].

§3. Émergence de la notion de cybercriminalité au sein des Nations Unies

Au début des années nonante, peu après les premières réglementations de l'O.C.D.E., c'est dans le contexte des Nations Unies que la notion de cybercriminalité fit son entrée[28].

Plusieurs principes directeurs furent établis à cette époque, mais l'étape la plus marquante de l'émergence de la notion de la cybercriminalité au sein des Nations Unies fut la création de la section UNDOC, *United Nations Office on Drugs and Crime* en 1997[29]. Cette section s'occupe de la criminalité organisée. La criminalité organisée exploite déjà pleinement les nouvelles technologies d'information et de communication et est dès lors un sujet de discussion récurrent au sein de cette section.

---

[24] Il s'agit du Canada, de la France, de l'Allemagne, de l'Italie, du Japon, de la Grande-Bretagne, des États-Unis et de la Russie.

[25] Union Internationale des Télécommunications, *Comprendre la Cybercriminalité : guide pour les pays en développement, op. cit.*, p. 103.

[26] Pour de plus amples informations à ce sujet, voy. Union Internationale des Télécommunications, *Comprendre la Cybercriminalité : guide pour les pays en développement, op. cit.*, pp. 103 à 106.

[27] Plus d'informations à ce sujet dans A. DEBAETS e.a, *op. cit.*, pp. 387 à 392. Voy. également les plans des différents sommets organisés par le G8, disponible sur : http://www.g8.utoronto.ca/summit/index.htm.

[28] Le thème de la cybercriminalité fut abordé au sein des Nations Unies pour la première fois durant le huitième Congres pour la prévention du crime et du traitement des délinquants, à La Havane du 27 août au 7 septembre 1990. Rapidement ceci fut suivi par divers manuels, décisions, résolutions et recommandations.
Pour plus informations, voy. Union Internationale des Télécommunications, *Comprendre la Cybercriminalité : guide pour les pays en développement*, UIT, Genève, 2009, pp. 106 à 108.

[29] K. VERHAEGHE, « Opsporing en vervolging in cyberspace », mémoire de master en droit, Université de Gand, 2011-2012, pp. 37 à 38.

L'utilisation du *dark-web* à des fins illégales[30], la vente de drogues et d'armes sur Internet ainsi que les communications cryptées sont des domaines dans lesquels les bandes criminelles organisées excellent. Selon certains rapports, le profit tiré de la criminalité informatique par la criminalité organisée est principal au profit que ces délinquants tirent du trafic de drogue[31].

La cybercriminalité reste donc une préoccupation centrale pour les Nations Unies. Annuellement plusieurs Congrès et Conférences sont organisés afin d'essayer que la société internationale se dote des outils nécessaires pour avoir une approche globale et cohérente de ce problème croissant[32].

Il convient aussi de signaler que l'Union Internationale des Télécommunications est une agence spécialisée des Nations unies. Celle-ci est également active dans la réflexion à propos de la lutte en matière de cybercriminalité[33].

§4. Émergence de la notion de cybercriminalité au sein du Conseil de l'Europe

La notion de cybercriminalité n'est pas étrangère au Conseil de l'Europe non plus, bien au contraire. C'est au sein du Conseil de l'Europe que fut élaboré la Convention de Budapest[34] qui est actuellement la seule convention internationale pour la lutte contre la criminalité informatique.

La création de la Convention de Budapest n'eut pas lieu en un jour, et la préoccupation concernant la cybercriminalité naquit bien avant 2001 au sein du Conseil de l'Europe. C'est déjà à la fin des années quatre-vingt que la préoccupation au niveau du Conseil de l'Europe devint plus grande. Deux recommandations, en 1989 et 1995, furent alors adressées aux états membres afin que ceux-ci établissent une liste d'infractions minimales et augmentent les

[30] Le *dark web* est bas-fond du réseau Internet, qui est difficilement accessible et sur lequel se produit tout type de marché noir, de trafic illégal et la commission de nombreux délits. On trouve la possibilité d'acheter de la drogue, des armes, des vidéos pédopornographique, des contacts de tueurs à gages, des recettes à base de viande humaine, plein d'autres articles illégaux.
L'utilisation du *dark web* ce fait de façon anonyme par un réseau appelé *The Onion Router*, qui en tant que tel, n'a rien d'illégal. Ce logiciel permet de masquer l'adresse IP de l'utilisateur par différents procédés complexes mêlant cryptage et connexions aléatoires à des serveurs.
[31] Voy. annexe n° 1, question 8 de la retranscription de l'interview avec l'inspecteur Koen SMETS et Marjolein DELPLACE.
[32] Plus d'informations à ce sujet dans A. DEBAETS e.a, *op. cit.*, pp. 398 à 407.
[33] Pour de plus amples informations en la matière, voy. le site web de l'Union Internationale des Télécommunications : http://www.itu.int.
[34] Convention sur la cybercriminalité, Conseil de l'Europe, signée à Budapest le 23 novembre 2001. Ci-après dénommée « Convention de Budapest ».

pouvoirs d'enquête dans le cyberespace[35]. Il ne s'agissait que de recommandations, sans effet obligatoire pour les États membres.

Au fil du temps, la nécessité d'une harmonisation se faisait croissante et pour cette raison le Conseil de l'Europe créa un comité d'experts chargés d'élaborer la Convention de Budapest qui vit le jour en 2001[36]. Cette convention est actuellement ratifiée par 47 états[37], membres ou non-membres du Conseil de l'Europe[38]. Quelques signatures ne sont à ce jour toujours pas suivies de ratification[39].

L'objectif principal de la Convention de Budapest est l'harmonisation des législations des états membres pour de permettre une lutte plus efficace contre la cybercriminalité. La Convention crée des incriminations-types que les états membres doivent insérer dans leur législation.

La Convention de Budapest est accompagnée d'un Protocole additionnel[40] afin de permettre à certains membres de la Convention d'aller plus loin dans l'harmonisation de la législation. Dans le cas précis, le Protocole fut purement réalisé pour permettre d'y insérer des dispositions que les États-Unis ne souhaitaient pas voir insérées dans la Convention de Budapest[41].

Section III. Contenu de la notion de cybercriminalité

Il n'est pas aisé de savoir ce que recouvre exactement la notion de cybercriminalité. La cybercriminalité étant un phénomène largement international, il serait logique de disposer d'une définition claire et universelle. Malheureusement, au jour d'aujourd'hui, aucune convention internationale ne la définit clairement et les législations nationales se contentent bien souvent

[35] Recommandation n° R (89) 9 sur la criminalité en relation avec l'ordinateur du 9 septembre 1989, adoptée le 13 septembre 1989, Editions du Conseil de l'Europe, Strasbourg, 1990, disponible sur http://www.coe.fr/cm/ta/rec/1989/f89r9.htm.
Recommandation n° R (95) 13 relative aux problèmes de procédure pénale liés à la technologie de l'informatique, adoptée le 11 septembre 1995, éditions du Conseil de l'Europe, 1996 disponible sur http://www.coe.fr/cm/ta/rec/1995/f95r13.htm.

[36] A. DEBAETS e.a.., *op. cit.*, p. 399.

[37] Données concernant la signature et la ratification de la Convention de Budapest de 2001 disponible sur : http://conventions.coe.int/Treaty/.

[38] En effet, certains pays comme les États-Unis, le Japon et le Canada ne sont pas membres du Conseil de l'Europe, mais l'ont signé et ratifié.

[39] Andorre, Grèce, Suède, Irlande ont signé mais pas ratifié la Convention.

[40] Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, 28 janvier 2003, Strasbourg, disponible sur : http://conventions.coe.int/Treaty/FR/Treaties/Html/189.htm.

[41] Le projet de convention comportait des dispositions sur le racisme et la xénophobie. Toutefois, les États-Unis ne souhaitaient pas être liés par ces dispositions, qu'ils jugeaient contraire à la liberté d'expression. Ainsi ces dispositions firent l'objet d'un protocole séparé. Pour plus d'informations à ce sujet voyez le rapport explicatif au premier protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, disponible sur : http://conventions.coe.int/Treaty/FR/Reports/Html/189.htm.

d'une énumération d'actes. Il reste donc difficile de savoir précisément ce que recouvre ce concept.

La première tentative de définition à vocation universelle de la notion de criminalité informatique fut réalisée par un groupe d'expert de l'O.C.D.E. en 1986[42]. Le groupe avait tenté de définir la délinquance informatique comme étant « tout comportement illégal ou contraire à l'éthique ou non autorisé qui concerne un traitement automatique de données et/ou une transition de données »[43].

Cette définition ne peut toutefois plus être acceptée aujourd'hui. À l'heure où le principe de légalité est une pierre angulaire de notre droit pénal, il ne peut être admis qu'un comportement soit érigé en infraction uniquement car il est contraire à l'éthique[44]. Pour qu'un comportement soit érigé en infraction, il doit être incriminé spécifiquement par le législateur. La définition de l'O.C.D.E. est donc trop large et viole le principe de légalité.

Les autres acteurs internationaux et de nombreux pays définissent souvent la cybercriminalité au moyen d'une énumération d'actes qui varient d'un pays à l'autre, ou d'une organisation à l'autre[45]. Ainsi, les contours exacts de la notion restent flous.

Toutefois, en combinant plusieurs approches, la doctrine permet de dégager quelques réponses quant à la définition de la cybercriminalité[46].

Il convient de combiner une approche sémantique et une approche juridique.

L'approche sémantique estime que pour faire partie de la cybercriminalité il faut que le comportement soit lié au cyberespace, « c'est-à-dire [à] l'espace cybernétique, à la communication en ligne, à la communication par voie électronique, aux réseaux de

[42] I. COLLARD, *op. cit.*, pp. 182 à 183.
[43] I. COLLARD, *op. cit.*, pp. 182 à 183.
[44] I. COLLARD, *op. cit.*, p. 183.
[45] Ainsi par exemple, la Convention sur la cybercriminalité du Conseil de l'Europe, signée à Budapest le 23 novembre 2001, ne définit pas non plus la cybercriminalité de manière claire mais a recours à une énumération d'actes. Le terme « cybercriminalité » est un concept « fourre-tout » dans lequel on regroupe toutes les infractions ayant un lien avec le cyberespace. La notion reste floue et seul au moyen d'une énumération d'infractions, on peut comprendre ce que la notion recouvre.
En droit belge également, c'est une liste d'infractions qui vient clarifier ce qu'il faut entendre sous le vocable criminalité informatique.
[46] J. FRANCILLON, « Cybercriminalité. Aspects de droit pénal international. – La société de l'information et le droit pénal », Actes du colloque préparatoire de Helsinki du 10-12 juin 2013 organisé par l'Association Internationale de Droit Pénal, *Revue Internationale de Droit pénal*, 2013, p. 4.

télécommunication »[47]. Le dénominateur commun de la criminalité informatique serait donc cet espace « virtuel, immatériel, en tout cas sans frontières, mondialisé et universel »[48].

L'approche juridique est l'approche retenue par la Convention de Budapest sur la cybercriminalité du 23 novembre 2001. Cette convention ne définit pas la notion de cybercriminalité mais apporte quelques éléments de réponses. Selon la Convention, la notion de cybercriminalité peut être comprise comme étant « les actes [qui portent] atteinte à la confidentialité, à l'intégrité et à la disponibilité des systèmes informatiques, des réseaux et des données ainsi que leur usage frauduleux »[49].

La notion de système informatique est quant à elle définie dans la Convention de Budapest comme étant « tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données » [50].

Il résulte de tout ce qui précède que bien que nous disposions de divers éléments permettant d'éclairer un peu la notion de cybercriminalité, il subsiste toutefois des zones d'ombres quant à son contenu précis.

Section IV. La classification de la cybercriminalité

La cybercriminalité est une notion relativement vaste qui recouvre de nombreuses infractions et de nombreuses réalités. Pour cela, le législateur, mais aussi la doctrine, ont élaboré différentes catégories au sein de la cybercriminalité afin d'y voir un peu plus clair.

Dans le cadre de ce mémoire, nous aborderons successivement les deux principales manières d'opérer des classifications au sein de la cybercriminalité. La première consiste en la distinction entre cybercriminalité spécifique et non-spécifique (§1). Dans la Convention de Budapest, le Conseil de l'Europe a, quant à lui, préféré une classification en quatre classes dans la Convention de Budapest (§2).

[47] *Ibidem*
[48] J. FRANCILLON, *op. cit.*, p. 1.
[49] J. FRANCILLON, *op. cit.*, p. 4 ; Ceci ressort également du préambule de ladite Convention de Budapest.
[50] Art. 1 de ladite Convention de Budapest.

§1. La classification de la cybercriminalité spécifique vs. non-spécifique

La délinquance informatique fut dans un premier temps vue comme une nouvelle forme de criminalité à part entière[51].

Néanmoins, de nos jours, il apparaît évident que la cybercriminalité n'est pas uniquement une nouvelle forme de criminalité mais peut se diviser en deux volets distincts : l'un étant neuf, l'autre faisant référence à la criminalité traditionnelle[52].

Premièrement, l'émergence de nouvelles technologies et surtout d'Internet permet la commission de délits qui n'étaient pas prévus dans l'arsenal législatif et qui sont intimement liés aux NTIC. Ces nouveaux délits prennent comme cible le système informatique. Il s'agit par exemple du *hacking*, de l'interception illégale de données, de l'atteinte à l'intégrité du réseau etc. Nous utiliserons le vocable « criminalité spécifique » chaque fois qu'une incrimination spécifique est prévue pour un comportement du cybermonde[53].

À côté de cette nouvelle forme de criminalité, une grande partie de la cybercriminalité est composée d'infractions classiques commises par le biais de nouvelles technologies, il s'agit alors de la cybercriminalité non-spécifique[54].

En effet, avec l'accès quasi-généralisé à Internet en Belgique[55] ainsi qu'avec le rôle accru des nouvelles technologies d'information et de communication dans la vie quotidienne des citoyens et des entreprises, de plus en plus d'infractions traditionnelles sont commises par le biais des NTIC. Les nouvelles technologies sont devenues un outil pour commettre des infractions traditionnelles. À titre d'exemple, nous pouvons retenir les cas très fréquents d'extorsions ou de harcèlements réalisés sur Internet, ainsi que les faits de pédopornographie présents également en grande quantité sur les réseaux.

---

[51] Conseil de l'Europe, *Criminalité organisée en Europe : la menace de la cybercriminalité, op. cit.,* p. 91.
[52] Conseil de l'Europe, *Criminalité organisée en Europe : la menace de la cybercriminalité, op. cit.,* p. 92.
[53] I. COLLARD, *op. cit.,* pp. 612 à 614.
[54] *Ibidem*
[55] En 2014, selon la Banque Mondiale, en Occident l'accès à Internet est quasi-généralisé. En Belgique par exemple, 82,2% de la population dispose d'un accès à Internet. Aux États-Unis, il s'agit d'un pourcentage de 84%. Des pays tels que le Danemark et la Finlande atteignent des pourcentages de plus de 90%. Rapport de statistiques sur le développement des télécommunications dans le monde et base de données de l'Union internationale des télécommunications et estimations de la Banque mondiale, disponible sur : http://donnees.banquemondiale.org/indicateur.

Dans le cadre de ce mémoire, nous utiliserons donc le terme de cybercriminalité non-spécifique chaque fois qu'une infraction, certes réalisée au moyen des NTIC, entre dans le champ d'application d'une infraction traditionnelle.

§2. La classification opérée par le Conseil de l'Europe

Cette classification de la cybercriminalité en deux volets, l'un spécifique et l'autre non-spécifique, n'est pas l'unique mode de classification des cyberdélits. La Convention de Budapest[56] classe les cyberdélits d'une autre manière. Elle distingue quatre types de cyberdélits.

En premier lieu, la Convention fait état des infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques[57]. Elle inclut dans cette catégorie les délits d'accès illégal, d'interception illégale, d'atteinte à l'intégrité des données, d'atteinte à l'intégrité des systèmes et d'abus de dispositifs.

En second lieu, il y a les infractions dites infractions informatiques traditionnelles telles que la fraude informatique et le faux en informatique[58].

En troisième lieu, la Convention retient les infractions se rapportant au contenu. Au sein de cette catégorie, l'on peut retrouver les offenses relatives à la pornographie enfantine[59].

Enfin, la Convention du Conseil de l'Europe crée une catégorie à part pour les infractions relatives aux atteintes à la propriété intellectuelle[60].

Cette classification opérée par le Conseil de l'Europe peut porter à confusion, en ce que les catégories se chevauchent partiellement et que de nombreux délits se retrouvent catalogués dans plusieurs d'entre elles[61]. Dans cette typologie, trois catégories se rapportent à l'objet de la protection juridique alors qu'une d'entre elles, la catégorie des infractions informatiques traditionnelles, se rapporte à la méthode[62]. Ceci crée donc une certaine incohérence.

Dans le cadre de ce mémoire, bien que quelques références soient faites à cette classification du Conseil de l'Europe, la classification entre infractions spécifiques et non-spécifiques de cybercriminalité sera préférée afin d'éviter les incohérences.

---

[56] Convention sur la cybercriminalité, Conseil de l'Europe, signée à Budapest le 23 novembre 2001.
[57] Art. 2 à 6 de ladite Convention de Budapest.
[58] Art. 7 à 8 de ladite Convention de Budapest.
[59] Art. 9 de ladite Convention de Budapest.
[60] Art. 10 de ladite Convention de Budapest.
[61] Union Internationale des Télécommunications, *Comprendre la Cybercriminalité : guide pour les pays en développement, op. cit.*, p. 20.
[62] *Ibidem*

Chapitre II. Les nécessités d'un cadre pénal pour la cybercriminalité

Comme mentionné précédemment, l'usage des nouvelles technologies et particulièrement d'Internet est à la hausse en Belgique, et dans le monde en général. En 2014, en Belgique, 83% des ménages disposent d'une connexion internet[63]. En seulement cinq ans, ce pourcentage a augmenté de près de dix pourcent[64].

Internet devient un outil indispensable et les avantages que cet outil offre aux particuliers et aux entreprises sont incommensurables. Les possibilités produites par un moyen de communication tel que celui-ci sont infinies. Mais ces possibilités infinies peuvent également être utilisées à mauvais escient par les cyberdélinquants.

L'accès quasi-généralisé à Internet a fait croître la cybercriminalité de manière incroyable. Les dernières années, la cybercriminalité semble augmenter de manière exponentielle[65]. En dix ans, le nombre d'infractions informatiques s'est multiplié par 18[66]. Le recours aux NTIC pour commettre des délits est devenu banal, à tel point qu'aujourd'hui le nombre de délits commis par le biais des nouvelles technologies est plus élevé que le nombre de délits traditionnels[67]. L'analyste stratégique du *Federal Computer Crime Unit*[68], M. Deplace, estime également que dans quasi tous les délits classiques, il y a maintenant un aspect « technologie »[69].

En 2011, une étude réalisée par *Norton by Symantec* révélait des statistiques à propos de la criminalité informatique, dont une image très parlante : trois belges par minute sont victimes de cybercriminalité[70]. Certaines victimes ne s'en rendent d'ailleurs jamais compte.

---

[63] Voy. annexe n° 6 afin de trouver le tableau complet des statistiques de StatBel, la direction statistique du SPF Économie, à propos de l'utilisation d'Internet auprès des ménages belges.
[64] Voy. annexe n° 8 pour les statistiques de StatBel à propos de l'utilisation des TIC auprès des ménages belges.
[65] Voy. annexe n° 9 pour les statistiques du ministère public sur le flux d'entrée des affaires de type « informatique » entre 2003 et 2014.
[66] Voy. annexe n° 9 pour les statistiques du ministère public sur le flux d'entrée des affaires de type « informatique » entre 2003 et 2014. Sur cette période, le nombre d'infractions de type « informatique » qui constituent le flux d'entrée au ministère public ont augmenté 18 fois, en passant de 1.034 infractions en 2003 à 18.892 en 2014.
[67] K. VERHAEGHE, *op. cit.*, p. 30. Les résultats de K. VERHAEGHE furent obtenus sur base du *Cybercrime Report*, 2011 de *Norton by Symantec*.
[68] Ci-après dénommé FCCU.
[69] Voy. annexe n°1 pour la transcription complète de l'interview de deux membres du FCCU : l'inspecteur principal Koen SMETS et l'analyste stratégique Marjolein DELPLACE.
[70] En effet, les résultats du *Norton Cybercrime Report* de l'année 2011 évalue que 1,4 million de belges furent victimes de cybercriminalité, en 2010. Ceci correspond à trois belges par minutes. Rapport de *Norton by Symantec disponible* sur : http://be.norton.com/cybercrimereport.

Le *Center for Strategic and International Studies* a publié, en juin 2014, un rapport scientifique afin d'établir les coûts de la cybercriminalité dans le monde[71]. Le centre estime que chaque année la criminalité informatique cause une perte mondiale d'approximativement 375 milliard de dollars[72]. Ce chiffre très élevé comporte les pertes directes et indirectes. Sous le vocable de « perte indirecte » il y a lieu d'entendre le coût du temps perdu à la recherche, la poursuite et la lutte contre la cybercriminalité. Par le vocable « perte directe », le *Center for Strategic and International Studies* vise le coût, mesurable en argent, du cyberdélit pour sa victime. Le dernier rapport de *Norton by Symantec,* qui date de 2011, estime que les pertes directes liées à la cybercriminalité s'élèvent à 113 milliard de dollars[73] soit près de 300 dollar par victime de cybercriminalité[74].

Ces rapports furent réalisés par des entreprises vendeuses de logiciels protégeant des systèmes informatiques et il convient dès lors de relativiser, dans une certaine mesure, la gravité de leurs propos. Néanmoins, il est nécessaire de prendre la menace au sérieux.

L'accroissement de la cybercriminalité ainsi que les pertes colossales causées par celle-ci, furent deux raisons pour lesquelles il était devenu nécessaire de réagir et de combler le vide juridique qui existait, en Belgique, mais aussi ailleurs.

Pour ces mêmes raisons, il est encore toujours nécessaire de continuer à améliorer les mesures mises en place pour lutter contre cette criminalité et de s'adapter sans cesse à cette réalité qui évolue, au risque de perdre définitivement la « bataille » contre les cybercriminels.

Chapitre III. Les textes en vigueur en Belgique

La cybercriminalité est présente, certes en faible quantité, depuis les années soixante mais ne fut l'objet de régulation en Belgique qu'à partir des années 2000[75]. Avant cette date, elle fut abordée dans quelques projets de lois ambitieux de 1988 qui n'ont jamais aboutis[76].

[71] Rapport disponible sur : http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf
[72] Rapport disponible sur : http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf
[73] Rapport de *Norton by Symantec* disponible sur : http://be.norton.com/cybercrimereport
[74] Rapport de *Norton by Symantec* disponible sur : http://be.norton.com/cybercrimereport
[75] La loi du 28 novembre 2000 relative à la criminalité informatique, *M.B.*, 3 février 2001 fut la première loi belge à intervenir en matière de cybercriminalité.
[76] CH. MEUNIER, *op. cit.*, p. 620.

La Belgique a réagi relativement tardivement à l'avènement de cette nouvelle forme de criminalité en comparaison avec ses voisins[77]. À cause de cette lenteur, avant l'entrée en vigueur de la loi du 28 novembre 2000, les juges belges devaient faire part de beaucoup d'ingéniosité pour lutter tant bien que mal contre la cybercriminalité, au détriment parfois du principe de légalité.

Nous aborderons successivement la situation en vigueur avant la loi du 28 novembre 2000 (Section I) et la situation actuelle (Section II).

Section I. Avant l'entrée en vigueur de la loi du 28 novembre 2000

Avant l'intervention législative en 2000, un vide juridique était responsable de l'impunité de nombreux cybercriminels (§1), la procédure pénale n'était pas adaptée à un environnement numérique (§2) et, en comparaison avec ses voisins, la Belgique faisait partie des mauvais élèves européens (§3).

§1. Un vide juridique causant l'impunité

Avant l'entrée en vigueur de la loi du 28 novembre 2000, ce que nous appelons la cybercriminalité non-spécifique ne posait pas de problèmes particuliers[78]. En effet, les dispositions de droit pénal matériel s'appliquaient aux infractions traditionnelles commises sur Internet, sans que le législateur ou le juge ne se pose de questions. Les questions qui seront traitées dans les prochains chapitres quant à l'adéquation du droit pénal traditionnel aux infractions traditionnelles commises au moyen des NTIC, n'étaient pas d'actualité.

Toutefois, un vide juridique se faisait fortement ressentir. Pour les infractions qui ont pour cible les NTIC et qui se réalisent nécessairement dans le cybermonde sans équivalent dans le droit pénal matériel traditionnel, à savoir la cybercriminalité spécifique, les juges étaient forcés d'avoir recours à des solutions juridiques plus farfelues les unes que les autres afin d'éviter l'impunité[79].

Les solutions juridiques créatives s'illustrent bien dans la fameuse affaire du *Belgian Information System by Téléphone*, également appelée « Affaire *BisTel* »[80]. En l'espèce, une

[77] La Suède fut le premier pays à se doter d'une législation prenant en compte la criminalité informatique en 1973 ; En Allemagne, une loi du 15 mai 1986 ; En France un loi du 5 janvier 1988 ; En Angleterre une règlementation dès le 29 août 1990 ; Aux Pays-Bas et en Italie, les premières lois furent introduites en 1993 et en Espagne en 1995.
[78] CH. MEUNIER, *op. cit.*, pp. 612 à 614.
[79] *Ibidem*
[80] En première instance, l'affaire *BisTel* : Corr. Bruxelles, 8 novembre 1990, *J.T.*, 1990, p.11.

personne s'était introduite frauduleusement dans un système informatique par le détournement d'un mot de passe[81]. En se procurant le mot de passe d'un ministre, elle s'était introduite dans le système informatique et avait ensuite changé le mot de passe, de sorte de le rendre inaccessible aux personnes qui y avaient normalement accès. Elle prit également connaissance de communications privées.

Le *hacking* n'était pas encore prévu par la législation pénale belge de l'époque[82]. Afin de tenter de réprimer les faits, le tribunal de première instance qualifia ceux-ci de faux en écriture et jugea les prévenus coupables[83]. En effet, le juge assimila l'introduction d'un faux mot de passe à un faux en écriture.

Sans surprise, la décision fut réformée en appel car elle ne répondait pas au principe de légalité en ce qu'elle opérait une analogie interdite entre le mot de passe et un écrit au sens de l'article 193 du Code pénal[84].

Le prévenu échappa donc à toute condamnation, pour ce fait, dû au vide juridique.

Une autre affaire bien connue est l'affaire *Redattack*[85]. Cette affaire illustre également le problème causé par le manque de législation en la matière. Malgré les constructions juridiques qui étaient réalisées par les tribunaux belges dans une tentative de punir des comportements qui n'étaient pas encore incriminés par la loi, le vide juridique subsistait et certains comportements n'étaient pas punissables.

Frans Devaere, mieux connu sous le pseudonyme *Redattack* s'était introduit dans les serveurs de Skynet utilisés par la banque Fortis en 1999. N'ayant aucune mauvaise intention, si ce n'est de prouver que les systèmes de sécurité n'étaient pas effectifs, l'homme envoya à différents journalistes des preuves selon lesquelles il s'était introduit dans lesdits systèmes informatiques. L'homme fut néanmoins poursuivi et ensuite jugé coupable sur base de l'ancien article 109*ter* D, 4° de ladite loi Belgacom[86].

En degré d'appel, l'affaire *BisTel* : Bruxelles, 24 juin 1991, *R.D.P.C.*, 1992, p. 340.

[81] CH. MEUNIER, *op. cit.*, pp. 612 à 614.

[82] Le *hacking* fut introduit dans 550*bis* du Code pénal avec la loi du 28 novembre 2000.

[83] Dans le présent mémoire nous ne parlerons pas des autres charges retenues contre le prévenu, à savoir vol d'énergie informatique et détournement de communications.

[84] CH. MEUNIER, *op. cit.*, pp. 615 à 616.
Le principe de légalité et ses corollaires seront abordés en profondeur dans la seconde partie de ce mémoire.

[85] Corr. Gand, 11 décembre 2000, *Computerr.*, 2001, vol. 2, pp. 84 à 89.

[86] Loi du 21 mars 1999 portant réforme à certaines entreprises publiques économiques, *M.B.*, 27 mars 1991.

Toutefois, Frans Devaere ne fut jugé coupable que de la prise de connaissance du mot de passe, du code pin et du *login*. Aucune infraction ne fut retenue pour la prise de connaissance d'autres données telles que par exemple les données bancaires qu'il s'était permis de consulter dans le système informatique de la banque Fortis. Ces données ne tombaient pas dans le champ d'application de la loi Belgacom et le prévenu échappa ainsi à une condamnation pour ces faits-là. En conséquence, des faits qui étaient considérés comme étant répréhensibles ne furent pas punis à cause du vide juridique.

Ces deux affaires illustrent bien que des « comportements attentatoires aux systèmes informatiques et aux données qu'ils traitaient restaient impunis, car la matérialité de leur exécution ne correspondait pas aux éléments constitutifs des infractions de droit commun »[87].

§2. Une procédure pénale non-adéquate

Un constat d'inadéquation pouvait également être dressé en ce qui concerne la procédure pénale. En effet, le monde des NTIC correspond à une réalité très différente de celle des réseaux et le Code d'instruction criminelle et les lois de procédure pénale n'étaient pas aptes à répondre à une réalité virtuelle et numérique. La nécessité d'une réforme se faisait ressentir. Il fallait agir plus rapidement, avec des mécanismes permettant une entraide internationale et il fallait de nouveaux moyens d'identifier les cybercriminels et de rechercher des preuves. Les principes traditionnels n'étaient plus adaptés.

§3. Un courant international se faisant pressant

Un courant international prônant la criminalisation de la criminalité informatique naquit grâce à de nombreux acteurs tels que l'O.C.D.E., le Conseil de l'Europe, l'ONU, le G8 et l'Association Internationale de Droit Pénal[88].

La Belgique ressentait aussi une certaine stigmatisation en la matière. Au milieu de tous ses voisins européens, elle était le mauvais élève qui ne disposait pas d'une législation adéquate[89].

---

[87] O. LEROUX, « Criminalité informatique », *Infractions contre les biens*, sous la direction de H.-D. BOSLY et CH. DE VALKENEER, Bruxelles, Larcier, 2008, p. 372.

[88] CH. MEUNIER, *op. cit.*, pp. 617 à 620.
L'influence internationale consiste principalement en deux recommandations du Conseil de l'Europe : La Recommandation n° R (89) 9 sur la criminalité en relation avec l'ordinateur du 9 septembre 1989, adoptée le 13 septembre 1989, Editions du Conseil de l'Europe, Strasbourg, 1990, disponible sur http://www.coe.fr/cm/ta/rec/1989/f89r9.htm ainsi que la Recommandation n° R (95) 13 relative aux problèmes de procédure pénale liés à la technologie de l'informatique, adoptée le 11 septembre 1995, éditions du Conseil de l'Europe, 1996 disponible sur http://www.coe.fr/cm/ta/rec/1995/f95r13.htm.

[89] La métaphore du « mauvais élève » fut utilisée pour la première fois en 2002 dans l'ouvrage T. VERBIEST et J. DERVAUX, « La criminalité informatique dans tous ses états », *TBH*, 2002, vol. 8, p. 60 cité dans T. INCALZA,

Cette pression au niveau international mena à l'accélération de la réforme législative en Belgique.

Section II. Depuis l'entrée en vigueur de la loi du 28 novembre 2000

Ces trois gros problèmes[90] poussèrent le législateur belge à réagir à travers l'adoption de la loi du 28 novembre 2000. Cette loi n'a pas pour objectif d'opérer une réforme en profondeur mais souhaite seulement combler les lacunes du droit pénal, sans toucher aux valeurs traditionnelles[91].

En ce qui concerne le droit matériel, la loi du 28 novembre 2000 ne se préoccupe pas de la criminalité non-spécifique[92]. En effet, les incohérences en cybercriminalité créées par le fait de faire rentrer dans le champ d'application matériel d'une infraction traditionnelle son pendant virtuel n'étaient pas à l'ordre du jour il y a quinze ans.

La loi se contente de créer trois grandes catégories d'infractions de cybercriminalité spécifique : le faux et l'usage de faux en informatique, la fraude informatique et les infractions contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données stockées, traitées ou transmises par ses systèmes[93]. La dernière catégorie d'infractions fait référence tant à la nouvelle infraction de sabotage informatique, qu'à l'infraction de l'accès non autorisé à un système informatique, mieux connue sous le nom de *hacking*[94].

Vu le peu de connaissance des parlementaires en la matière, le *Federal Computer Crime Unit* fut consulté afin de faire de cette réforme, une réforme adéquate et permettant d'embraser la quasi-totalité des comportements nuisibles réalisés dans le monde virtuel[95].

En ce qui concerne la procédure pénale, la loi prévoit quelques nouveaux principes qui s'appliquent à la cybercriminalité dans son ensemble – spécifique et non-spécifique. Ces articles permettent d'adapter la procédure pénale classique à la réalité numérique.

« Strafonderzoek in het digitale tijdperk : zoeking en inbeslagneming », *Jura Falconis Jg.*, 2010-2011, vol. 2, p. 330.

[90] Le vide juridique, la procédure pénale inadéquate et la pression internationale.

[91] Projet de loi du 28 novembre 2000 relative à la criminalité informatique, exposé des motifs, *Doc. Parl.*, Chambre, n° 0213/001.

[92] En ce qui concerne le faux en informatique, on peut admettre que la loi du 28 novembre 2000 crée une infraction spécifique qui a un pendant traditionnel : le faux en écriture. Avec la création d'une infraction spécifique, l'infraction de faux en informatique rentre dès lors dans le champ d'application de la cybercriminalité spécifique et on échappe à l'utilisation du faux en écriture pour ses pendants numériques.

[93] F. DE VILLENFAGNE et S. DUSOLLIER, « La Belgique sort enfin ses armes contre la cybercriminalité : à propos de la loi du 28 novembre 2000 sur la criminalité informatique », *A&M*, 2001, n°1, p. 60.

[94] *Ibidem*

[95] *Ibidem*

Depuis la réforme de 2000, une seule grande réforme a eu lieu, par la loi du 15 mai 2006[96]. Cette loi a modifié les articles 259*bis* 314*bis*, 504*bis*, 550*bis* et 550*ter* du Code pénal afin d'améliorer les textes en vigueur et de les mettre en adéquation avec la Convention de Budapest du Conseil de l'Europe. Cette réforme a principalement eu comme conséquence d'accroître la pénalisation de la criminalité informatique[97].

Les dispositions réglant la criminalité informatique auront bientôt quinze ans d'âge. Dans les prochaines parties de ce travail, nous analyserons ces dispositions afin de savoir si tant d'un point de vue matériel que procédural, ces dispositions sont (encore) efficaces.

[96] Loi du 15 mai 2006 modifiant les articles 259*bis* 314*bis*, 504*bis*, 550*bis* et 550*ter* du Code pénal, *M.B.*, 12 septembre 2006.
[97] KEUSTERMANS, J. et DE MAERE, T., « Tien jaar wet informaticacriminaliteit », *R.W.*, 2010-2011, n° 14, p. 564.

PARTIE II. DROIT PÉNAL MATÉRIEL DE LA CYBERCRIMINALITÉ

Dans cette seconde partie, une analyse sera faite du droit pénal matériel de la cybercriminalité non-spécifique (Titre I) et spécifique (Titre II) qui nous permettra d'avoir un avis éclairé quant à l'efficacité du droit pénal matériel relatif à la criminalité informatique.

TITRE I. LA CYBERCRIMINALITÉ NON-SPÉCIFIQUE

Comme nous l'avons vu, la cybercriminalité spécifique et non-spécifique ne sont pas traitées de la même manière en droit belge. Alors qu'au travers de la loi du 28 novembre 2000, le législateur belge a établi des infractions spécifiques pour les nouvelles infractions nées de l'essence même des nouvelles technologies, les infractions commises sur les NTIC qui ont un pendant traditionnel, ne bénéficient pas d'un encadrement juridique propre. En effet, le droit belge continue à se baser sur les infractions traditionnelles définies dans le Code pénal pour la plus grande majorité des infractions traditionnelles commises par le biais des NTIC[98].

Dans le présent titre nous n'aborderons pas toutes les différentes infractions comprises dans le vocable de cybercriminalité non-spécifique, en ce qu'elles sont innombrables vu qu'il s'agit de toutes les infractions traditionnelles réalisées par le moyen des nouvelles technologies. Nous nous limiterons à aborder les problèmes de violations potentielles du principe de légalité (Chapitre I) et de ses corollaires (Chapitre II). Ensuite, nous démontrerons ceci à travers certaines infractions (Chapitre III).

Ce Titre I permettra en définitive de déterminer s'il faut continuer d'assimiler les différentes infractions traditionnelles commises au travers des nouvelles technologies, aux infractions classiques du Code pénal ou si, inversement, il faudrait considérer la cybercriminalité comme un décor d'infractions nouvelles et indépendantes pour lesquelles il faudrait prévoir un volet spécifique au sein du Code pénal.

[98] Le droit belge comporte une infraction nouvelle qui a un pendant en droit traditionnel : il s'agit du faux en écriture dont le pendant numérique n'est pas puni par le faux en écriture mais par la nouvelle infraction de faux en informatique.

Chapitre I. Le principe de légalité

Le monde des télécommunications est un monde qui est en évolution constante et qui voit naître des comportements de plus en plus complexes et difficilement définissables. En continuant de sanctionner ces nouveaux comportements par les infractions traditionnelles du Code pénal de 1867 – époque où la technologie n'existait pas – il y a un gros risque de violation du principe de légalité et de deux de ses corollaires.

Le principe de légalité est un principe fondamental du droit pénal qui nous vient directement de l'adage latin *nullum crimen sine lege, nulla poena sine lege*[99]. Il résulte de cet adage, que les incriminations et les peines doivent être prévues par une loi, claire et précise.

Le principe de légalité revêt une importance capitale dans notre ordre juridique et est consacré dans la Constitution aux articles 12 et 14[100] ainsi que dans la Convention de sauvegarde des droits de l'homme et des libertés fondamentales à l'article 7§1[101].

Ce principe, dans un sens formel, veut que seul le « pouvoir législatif [dispose de] la compétence d'une part, de déterminer dans quels cas et dans quelle forme des poursuites sont possibles, d'autre part, d'adopter la loi en vertu de laquelle une peine peut être établie et appliquée »[102].

En d'autres mots, ce principe dans son sens formel signale que le pouvoir d'incrimination appartient uniquement au législateur et que « le juge ne peut incriminer des faits qui ne sont pas qualifiés d'infraction par la loi, quelle que soit son opinion sur leur moralité ou leur dangerosité »[103]. Il ne peut pas non plus prononcer de peine qui ne soit pas prévue par la loi. Ce principe découle du principe de la séparation des pouvoirs.

Dans un sens substantiel, le principe de légalité promeut la sécurité juridique en exigeant que la loi pénale soit claire et précise[104]. Il faut donc qu'en prenant connaissance de la loi pénale,

---

[99] F. TULKENS e.a., *Introduction au droit pénal. Aspects juridiques et criminologiques*, Bruxelles, Kluwer, 9e éd., 2010, p. 223.
[100] Constitution, art. 12 et 14.
[101] CEDH, art. 7§1.
[102] C.A., 30 janvier 1999, *Rev. dr. pén. crim.*, 1999, p. 808.
Toutefois, l'expression « en vertu de la loi » utilisée par le législateur dans l'article 14 de la Constitution permet une certaine délégation au Roi dans des cas restreints.
[103] F. TULKENS e.a., *op. cit.*, p. 226.
[104] F. TULKENS e.a., *op. cit.*, p. 228.

toute personne puisse savoir si le comportement qu'elle adopte est constitutif d'une infraction[105].

La Cour européenne des Droits de l'Homme accepte que certains termes plus vagues puissent être utilisés dans la législation pénale à condition que « le justiciable puisse savoir […] au besoin à l'aide de l'interprétation qui en est donnée par les tribunaux, quels actes et omissions engagent sa responsabilité pénale »[106].

Ce principe est considéré comme un des principes fondamentaux du droit pénal, en Belgique, mais également dans de nombreux autres pays.

Chapitre II. Les corollaires au principe de légalité

En droit pénal, le principe de légalité comporte trois corollaires. Le premier est le principe de non-rétroactivité du droit pénal. Celui-ci n'a que peu de pertinence dans le cadre de ce mémoire et ne sera donc pas abordé. Les deux autres corollaires sont, d'une part, le principe d'interprétation stricte de la loi pénale (Section I) et, d'autre part, l'interdiction d'interprétation par analogie de la loi pénale (Section II).

Section I. Le principe d'interprétation stricte de la loi pénale

Le principe d'interprétation stricte de la loi pénale est une directive générale d'interprétation découlant du principe de légalité ainsi que du caractère exceptionnel du droit pénal[107].

Ce principe exclut que le juge s'immisce dans la fonction législative et que, sous le prétexte d'une lacune de la loi, celui-ci affirme « rechercher l'intention du législateur afin de suppléer à son oubli ou procéder à l'application des lois d'incrimination ou de pénalité par analogie »[108].

Comme le rappelle F. Kuty, « il est, soit dit en passant, paradoxal, en droit pénal, de parler de lacune. Le comportement est ou non incriminé par la loi et, s'il ne l'est pas, c'est parce que le législateur n'a pas, ou pas encore, estimé devoir le faire »[109] et ce n'est pas au juge d'accroître

[105] M. NIHOUL, « A propos de la précision requise pour définir une infraction en vertu du principe de légalité ou de prévisibilité du droit pénal », *J.T.*, 2004, p.2.
[106] Cour eur. D.H., arrêt Radio France et autres c. France, 30 mars 2004, req. n° 53984/00, §20.
[107] F. TULKENS e.a., *op. cit.*, p. 294.
[108] F. KUTY, *Principes généraux du droit pénal belge,* tome 1, Bruxelles, Larcier, 2009, p. 197.
[109] *Ibidem*

le champ d'application du droit pénal en raison du principe de légalité et de séparation des pouvoirs.

En droit romain déjà, le principe *odiosa sunt restringenda* était d'application et voulait que les lois restrictives de droits et libertés soient d'interprétation stricte[110]. Le principe est resté d'application et est aujourd'hui une des pierres angulaires du droit pénal belge mais également international. En effet, la Cour européenne des Droits de l'Homme, dans l'arrêt *Mattei c. France*, s'est exprimée à propos de ce principe en affirmant « son attachement au principe de l'interprétation stricte du droit pénal »[111].

Dès lors, tant en droit belge qu'en droit international, il convient de respecter ce principe selon lequel le juge ne peut pas donner une interprétation autre – ou plus large – à la loi que celle que le législateur lui a donnée.

Section II. L'interdiction d'interprétation par analogie de la loi pénale

Un autre corollaire du principe de légalité est l'interdiction d'interprétation par analogie de la loi pénale[112].

L'interprétation par analogie consiste en l'interprétation extensive d'une règle de droit de façon à inclure dans son champ d'application matériel des situations qui ne sont pas visées par la règle bien qu'elles possèdent certaines similitudes avec les situations relevant du champ d'application de celle-ci[113].

Bien entendu, afin de respecter le principe de légalité, l'interprétation par analogie est interdite. L'interdiction n'est pas consacrée dans la loi, mais la jurisprudence de la Cour de cassation l'a affirmé très clairement[114]. Toutefois, la jurisprudence belge admet l'interprétation analogique de la loi pénale favorable au prévenu[115].

Il convient de distinguer l'interprétation analogique de l'interprétation dite évolutive qui est permise en droit belge[116]. L'interprétation évolutive permet d'inclure dans le champ

[110] F. TULKENS e.a., *op. cit.*, p. 296.
[111] Cour eur. D.H., arrêt Matei c. France, 19 décembre 2006, req. n° 34043/02.
[112] Le principe d'interdiction d'interprétation analogique de la loi pénale est un corollaire du principe de légalité mais également du principe d'interprétation stricte de la loi pénale.
[113] F. TULKENS e.a., *op. cit.*, pp. 296 à 297.
[114] L'affirmation du principe fut réitérée en 2005 de façon claire par la Cour de cassation dans l'arrêt Cass., 29 juin 2005, *Pas.*, 2005, p. 1470. « Attendu que le juge ne peut étendre une loi pénale par voie d'analogie à un cas qu'elle ne vise pas expressément ».
[115] F. KUTY, *op. cit.*, pp. 240 à 241.
[116] F. TULKENS e.a., *op. cit.*, pp. 297 à 298.

d'application matériel d'une règle pénale des faits à propos desquels « la volonté du législateur d'ériger des faits de cette nature [est] certaine et que ces faits [peuvent] être compris dans la définition légale de l'infraction »[117].

Il faut donc, pour que l'on puisse parler d'interprétation évolutive, que trois éléments soient réunis. Premièrement, il faut qu'à tout moment la définition légale de l'infraction soit respectée[118]. Il faut ensuite qu'il eut été impossible pour le législateur d'envisager le comportement litigieux au moment de la rédaction du texte législatif. Enfin, la jurisprudence requiert qu'il y ait une certitude quant à la volonté du législateur d'incriminer ce comportement litigieux, s'il avait pu en avoir connaissance[119].

Chapitre III. Analyse du respect de ces principes au regard de quelques infractions

Dans ce chapitre nous analyserons le cas le plus flagrant de violation du principe de légalité et de deux de ses corollaires à travers l'infraction du « vol » de données informatiques (Section I) et nous nous pencherons ensuite sur d'autres infractions requérant la matérialité de leur objet (Section II).

Section I. Le cas d'école : le « vol » de données

Un « vol » de données commis au moyen de NTIC ne rentre pas dans le champ d'application matériel des nouvelles infractions de cybercriminalité spécifique mais est, à l'heure d'aujourd'hui, toujours puni comme un vol de droit commun[120].

Un « vol » de données peut se matérialiser de diverses façons. La plus connue est l'introduction d'un dispositif de stockage[121] dans un ordinateur afin d'y copier des données et autres informations, sans disposer de l'autorisation de copier celles-ci.

---

[117] Cass., 2 octobre 2002, *Pas.*, 2002, p. 1796.
[118] F. KUTY, *op. cit.*, pp. 233 à 241.
[119] F. KUTY, *op. cit.*, pp. 240 à 241.
[120] Un seul cas de vol de données fut prévu spécifiquement par le législateur : le vol de données dans le cadre d'un *hacking*, qui est une circonstance aggravante de celui-ci. Hors ce cas d'espèce, aucune encadrement juridique spécifique n'est prévu.
La jurisprudence punit encore aujourd'hui le « vol » de données informatiques comme un vol traditionnel, bien que certaines juridictions ont émis des jugements allant en sens contraire. Voy. en ce sens, Verviers, 4 octobre 1989, *J.L.M.B.*, 1990, p. 709 ; Liège, 25 avril 1991, *R.D.P.*, 1991, p. 1013.
[121] Par exemple clé USB, disquette, CD, disque dur externe…

Un fait tel que celui-ci serait actuellement puni comme étant un vol, de droit commun. Bien entendu, le fait pourrait également être considéré comme une infraction aux droits d'auteurs, mais dans certains cas seulement[122].

De nombreux indices portent à croire qu'en retenant la qualification de vol de droit commun pour un fait de copie de données, sans en disposer de l'autorisation, le principe de légalité s'en trouverait violé.

L'article 461 du Code pénal prévoit que le vol est « la soustraction frauduleuse d'une chose appartenant à autrui ».

Le premier élément constitutif de la définition du vol donnée par le Code pénal[123] est le fait qu'il faut qu'il s'agisse d'une *chose*. Le vocable *chose*, en droit belge, s'utilise lorsqu'il s'agit d'un bien matériel. La chose matérielle est susceptible d'appropriation et de soustraction tandis que ceci, dans le cas d'une chose immatérielle, est impossible[124].

Des données sont des biens immatériels et ne seraient donc pas, dans la conception du Code pénal, susceptibles de soustraction. Seul le vol de données qui se trouvent déjà sur un support matériel pourrait donc être qualifié de vol[125].

Toutefois, il convient de nuancer le propos selon lequel seule une chose matérielle serait susceptible de vol[126]. En effet, dans certains cas, la jurisprudence belge a admis la qualification de vol pour des choses immatérielles. Le cas du vol d'électricité en est l'exemple le plus clair. Suite à un long débat, l'électricité fut considérée comme étant une *chose*. La Cour de cassation belge a en effet emboîté le pas à la Cour de cassation française et admis qu'un bien immatériel tel que l'électricité soit considéré comme une *chose*[127].

On pourrait admettre un même raisonnement dans ce cas-ci et appliquer cette qualification aux données informatiques. Ceci reste cependant critiquable. B. Frydman, chercheur en philosophie

[122] Ceci serait uniquement protégé par la législation sur les droits d'auteurs s'il s'agit d'une photo, d'un document etc. mais pas s'il s'agit de *data.*
[123] Code pén., art. 461.
[124] M. BRAUN, « Les infractions en matière de cybercriminalité », *J.T.L.*, 2011, n° 18, pp. 141 à 154.
[125] L'objet du vol serait alors la chose matérielle sur laquelle se trouvent des données, par exemple un CD ou une clé USB. Il y a donc vol si des données sont copiées d'un ordinateur sur un dispositif de stockage appartenant au propriétaire des données. Toutefois, si un « voleur » utilise son propre dispositif de stockage et y copie les données, il n'y a pas soustraction d'un objet matériel et en notre sens, pas de vol.
[126] C. ALLEAUME, « Les biens numériques, une notion au service du droit ? », Les technologies de l'information au service des droits : opportunités, défis, limites, sous la direction de D. LE MÉTAYER, Cahiers du CRID n°32, Bruxelles, Bruylant, 2010, p. 66.
[127] Cass., 23 septembre 1981, *Pas.*, 1982, p. 123.

du droit à l'Université Libre de Bruxelles, estime que le fait de considérer de l'électricité comme une chose est plus facilement acceptable que de le faire pour des données informatiques[128].

Selon lui, l'électricité peut être considérée comme une *chose* en ce qu'elle est, tout comme l'eau, « transportée par canaux chez les utilisateurs dans des quantités mesurables par compteur »[129]. Il s'agit là d'un processus métaphorique. Par contre le « vol » de données n'obéit pas à un processus métaphorique mais bien métonymique[130]. C'est-à-dire qu'on opère une analogie entre la chose et les données en assimilant « l'objet convoité (les données) au support sur lequel celles-ci sont copiées (disque ou disquette) pour pouvoir constater une soustraction matérielle […] »[131]. Ainsi « La jurisprudence belge qui assimile le vol de données informatiques à un vol d'électricité repose sur une métonymie : l'opération ne porte pas sur l'électricité elle-même ou sur une chose qui lui ressemblerait mais est bien commis à l'aide de l'électricité, énergie qui assure le fonctionnement des ordinateurs »[132]. Le discours scientifique nous enseigne qu'alors que la métaphore est perçue comme mode de pensée rationnel, la métonymie ne l'est pas[133]. Ceci serait en argument en faveur de la création d'une infraction spécifique pour le vol de données, car il ne serait pas acceptable d'identifier des données à une chose matérielle.

Toutefois, même dans le cas où l'on admettrait que des données puissent être vues comme une chose matérielle[134], d'autres éléments de définitions posent également problème.

En effet, une autre difficulté existe en ce qui concerne le second élément constitutif de la définition de vol : la *soustraction.* Pour qu'il y ait soustraction, il faut que les données volées disparaissent de l'ordinateur du propriétaire des données. Toutefois, « en matière de ce que l'on appelle improprement « vol d'informations », [le fait se réalise] par un accès indu à un système informatique [et] il n'y a pas de soustraction d'un bien quelconque ni d'appréhension […] étant donné que par le fait d'interroger un ordinateur on ne soustrait ou n'appréhende aucune donnée ou bien immatériel quelconque, puisque celui-ci demeure intact dans le système, et que le manipulateur n'a à aucun moment la possession exclusive du bien en question »[135].

---

[128] B. FRYDMAN, « Les formes de l'analogie », *Analogie et méthodologie juridique, R.R.J.*, Presses Universitaires d'Aix-Marseille, 1995, pp. 1060 à 1062. Disponible sur : http://www.philodroit.be/Les-formes-de-l-analogie
[129] B. FRYDMAN, *op. cit.*, p. 1061.
[130] *Ibidem*
[131] *Ibidem*
[132] *Ibidem*
[133] *Ibidem*
[134] Certains auteurs en sont déjà convaincus. Voy. en ce sens : C. ALLEAUME, *op. cit.*, pp. 66 à 68.
[135] Travaux parlementaires n°349, avis du Conseil d'état Luxembourgeois, pp. 12 à 13, cité dans M. BRAUN, *op. cit.*, pp. 141 à 154.

En conséquence, en appliquant l'infraction de « vol » à des faits qui ne remplissent pas la définition légale de cette dernière, on méconnaît le principe de légalité dans son sens formel selon lequel seul le législateur est habilité à incriminer des comportements.

Ceci fut confirmé par la Cour de cassation en 2004[136]. Il ressort de cet arrêt que le fait de faire une copie illégale de données, n'est pas constitutif de vol. J. Deene souligne que dans un vol il est impératif de s'approprier le bien d'autrui de sorte que le propriétaire d'origine n'en bénéficie plus, ce qui n'est pas le cas lors d'une copie illégale[137].

Une solution possible serait d'adapter la définition traditionnelle du vol afin de permettre qu'une *copie* d'un bien *immatériel* puisse entrer dans le champ d'application mais on prendrait alors le risque de trop élargir cette infraction traditionnelle.

La France a trouvé une solution à ce problème. L'article 323-3 du Code pénal français permet de punir le vol de données par copie. Ce dernier est compris dans l'infraction de fraude informatique. L'article sanctionne « le fait d'introduire frauduleusement des données dans un système de traitement automatisé, *d'extraire, de détenir, de reproduire*, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient »[138].

Toutefois, en Belgique, l'ajout des mots « extraire, détenir, reproduire » dans la définition de la fraude informatique ne serait qu'une solution partielle. Contrairement à l'infraction de fraude informatique française, la fraude informatique belge requiert la procuration d'un avantage économique illégal. Or, rien n'empêche qu'un « vol » de données soit réalisé sans qu'il ne procure un avantage économique illégal au « voleur ».

Au Luxembourg, la question du « vol » de données est également au cœur de l'actualité. Le Conseil d'état luxembourgeois s'est toujours prononcé en faveur de la création d'une infraction propre pour le délit de vol de données[139] en estimant que l'infraction traditionnelle était incapable de remplir les conditions pour rentrer dans le champ d'application de l'infraction traditionnelle[140].

---

[136] Cass., 30 novembre 2004, cité dans J. DEENE, « Illegaal kopiëren is geen diefstal », *Juristenkrant*, 2005, n° 102, p. 11.
[137] J. DEENE, « Illegaal kopiëren is geen diefstal », *Juristenkrant*, 2005, n° 102, p. 11.
[138] Code pén. français, art. 323-3.
[139] J.-L. PUTZ, « Observations », note sous Cour d'appel (5e ch.), 19 février 2013, *J.T.L.*, 2013, n°23, pp. 81 à 84.
[140] Toutefois, il est peu probable qu'une nouvelle infraction voit le jour car la Cour de Cassation a récemment déclarée que des biens incorporels peuvent être volés. Voy. l'arrêt de la Cour de Cassation Luxembourgeoise, 3 avril 2014, n°17/2014, *DAOR*, n°111, 2014, pp. 156 à 166.

Selon nous, la seule solution satisfaisante en droit belge est donc d'insérer une infraction à part entière pour le « vol de données » dans le Code pénal avec une définition permettant de comprendre dans son champ d'application la copie de données. Ceci permettrait d'avoir une infraction commune pour tous les types de vols de données et d'éviter d'avoir recours, dans certains cas, à l'infraction traditionnelle, dans d'autres, à l'infraction de *hacking* ou encore à d'autres législations[141].

Section II. Les autres délits supposant une atteinte à un bien matériel

Le raisonnement tenu dans la section précédente s'applique *de facto* par analogie à d'autres délits requérant *une chose* comme élément constitutif.

Nous avons fait le choix, dans le cadre de ce mémoire de nous limiter à citer quelques exemples, étant donné le raisonnement similaire à la remarque concernant l'immatérialité des données[142].

Nous pouvons retenir à titre d'exemple le cas de l'abus de confiance[143]. L'abus de confiance vise la situation dans laquelle une personne ayant reçu une chose d'une certaine matérialité, le détourne ou le dissipe.

L'article 491 du Code pénal dresse une liste exhaustive[144] des biens pouvant faire l'objet d'un abus de confiance. Cette liste fait état de « effets, deniers, marchandises, billets, quittances [ainsi que d'] écrits de toute nature contenant ou opérant obligation ou décharge »[145]. Les données informatiques qui sont dépourvues de toute matérialité ne sont pas reprises dans cette liste exhaustive.

De plus, celles-ci ne peuvent pas non plus entrer dans le vocable « écrits de toute nature » étant donné qu'il fut jugé dans la célèbre affaire *BisTel* que des données ne sont pas constitutives d'un écrit au sens du droit pénal traditionnel[146].

---

[141] Par exemple la législation relative à la propriété intellectuelle.
[142] Pour un raisonnement en profondeur, voy. la section I sur le « vol » de données informatiques.
[143] Code pén., art. 491.
[144] Cass., 5 janvier 2011, *R.D.P.C.*, 2011, p. 584. « Les choses mobilières sur lesquelles peut porter l'abus de confiance sont celles qu'énumère limitativement l'article 491 du Code pénal ».
[145] Code pén., art. 491.
[146] Bruxelles, 24 juin 1991, *R.D.P.C.*, 1992, p. 340. Pour plus d'informations, voy. CH. MEUNIER, *op. cit.*, pp. 615 à 616.
Toutefois, il convient de noter qu'un arrêt de la Cour de cassation du 5 janvier 2011 accepte que certaines données informatiques peuvent dans certains cas « être assimilées aux écrits de toute nature ou autres objets mobiliers corporels visés par l'article 491 du Code pénal ». Cass., 5 janvier 2011, *R.D.P.C.*, 2011, p. 584.

À travers cet exemple, nous voyons qu'il y a un risque de violation du principe de légalité dans le cas où l'on utilise l'infraction traditionnelle pour punir des comportements similaires commis par le biais des nouvelles technologies. Une adaptation législative reste dès lors souhaitable.

Un autre délit problématique est celui de l'extorsion[147]. Les objets de l'infraction d'extorsion sont « soit des fonds, valeurs, objets mobiliers, obligations, billets, promesses, quittances, soit la signature ou la remise d'un document quelconque contenant ou opérant obligation, disposition ou décharge ».

Certains auteurs estiment que cette liste exhaustive ne comprend pas les données informatiques[148] et qu'il y a donc violation du principe de légalité lorsque l'on applique l'infraction d'« extorsion » de données informatiques. Toutefois, il nous semble que dans certains cas les données informatiques pourraient être comprises sous le vocable « valeurs » en ce qu'elles peuvent avoir une valeur économique non négligeable. La question reste controversée.

[147] Code pén., art. 470.
[148] J.-L. PUTZ, *op. cit.*, pp. 83.

TITRE II. LA CYBERCRIMINALITÉ SPÉCIFIQUE

La loi du 28 novembre 2000 a introduit trois grandes catégories d'infractions de cybercriminalité spécifique : le faux et l'usage de faux en informatique (Chapitre I), la fraude informatique (Chapitre II) et enfin, les infractions contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données stockées, traitées ou transmises par ces systèmes (Chapitre III).

Chapitre I. Le faux et l'usage de faux en informatique

Le faux et l'usage de faux en informatique furent introduits à l'article 210*bis* du Code pénal. Dans un premier temps, nous analyserons les raisons pour lesquelles l'introduction de cette infraction fut nécessaire (Section I). Nous nous pencherons ensuite sur la définition et les éléments constitutifs de cette infraction (Section II) et nous terminerons par l'analyse des différents problèmes posés par celle-ci (Section III).

Section I. La nécessité d'une infraction de faux en informatique

L'instauration de l'infraction de faux en informatique fut nécessaire parce qu'en retenant le traditionnel faux en écriture classique pour des infractions commises par le biais des NTIC, le principe de légalité fut violé, selon la majorité de la doctrine[149].

Ceci fut également confirmé par la Cour d'appel de Bruxelles dans le fameux arrêt *BisTel*[150].

Un autre arrêt bien connu[151] illustre également la violation du principe de légalité et la nécessité d'instaurer cette nouvelle infraction de faux en informatique. Dans ce cas précis, une personne A avait créé une adresse imaginaire et l'avait utilisée dans un forum de discussion à caractère sexuel en se faisant passer pour personne B et avait proposé, sous ce nom, des services sexuels. Le numéro réel de la personne B figurait dans la fausse proposition de services sexuels et cela mena à un harcèlement téléphonique. Ces messages furent qualifiés par le tribunal de première instance de Liège de faux en écriture et usage de faux[152].

---

[149] O. LEROUX, « Le faux en informatique », *J.T.*, 2004, n° 6140, pp. 509 à 510 ; CH. MEUNIER, *op cit.*, p. 30 ; S. EVRARD, « La loi du 28 novembre 2000 relative à la criminalité informatique », *J.T.*, 2001, pp. 241 à 241.
[150] Bruxelles, 24 juin 1991, *R.D.P.C.*, 1992, p. 340.
[151] Civ. Liège (12e ch. corr.), 18 novembre 2002, *R.D.T.I.*, 2003, pp. 95 à 97.
[152] Civ. Liège (12e ch. corr.), 18 novembre 2002, *R.D.T.I.*, 2003, pp. 95 à 97.

Ce choix de qualification est critiquable en ce que les éléments constitutifs de l'infraction ne semblent pas être réunis[153]. En effet, une écriture, en droit commun, se compose des quatre éléments suivants : une « écriture matérielle, étant l'expression d'une pensée, ayant un contenu juridiquement relevant et bénéficiant de la confiance collective »[154].

O. Leroux et F. de Villenfagne qui ont commenté la décision du tribunal[155] déclarent que deux éléments constitutifs de l'infraction sont manquants dans le cas d'espèce. En effet, selon eux, « dans un forum de discussion à caractère sexuel où la plupart des gens se présentent sous un pseudonyme »[156], on ne peut parler ni d'écriture matérielle, ni de tromperie de la confiance collective[157].

À travers ces arrêts, l'on ressent clairement la nécessité qu'il y avait d'instaurer une nouvelle infraction de faux en informatique, pour permettre une répression efficace de ces nouveaux comportements. L'introduction de l'infraction de faux en informatique fit taire les débats quant au fait de savoir si une modification de data sur Internet constituait ou non une falsification d'*écriture*.

Section II. Définition et éléments constitutifs

Le faux et l'usage de faux en informatique furent introduits dans le Code pénal à l'article 210*bis* par la loi du 28 novembre 2000 afin de punir « celui qui commet un faux, en introduisant dans un système informatique, en modifiant ou effaçant des données, qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation possible des données dans un système informatique, et par là modifie la portée juridique de telles données »[158]. L'usage de ce faux est également incriminé.

Ceci signifie donc que « toute falsification, par le biais de la manipulation de données informatiques pertinentes »[159] et l'usage de celle-ci est désormais considéré comme un faux en informatique ou un usage de faux en informatique.

---

[153] F. DE VILLENFAGNE, « Chronique de jurisprudence 2002-2008. Criminalité informatique », *R.D.T.I.*, n° 39, 2010, p 12.
[154] *Ibidem*
[155] O. LEROUX, « Vers un premier faux informatique », obs. sous Civ. Liège (12e ch. corr.), 18 novembre 2002, *R.D.T.I.*, 2003, p. 97.
[156] F. DE VILLENFAGNE, *op. cit.*, p 12.
[157] O. LEROUX, « Vers un premier faux informatique », *op. cit.*, p. 97. Voy. également F. DE VILLENFAGNE, *op. cit.*, p. 12.
[158] Code pén., art. 210*bis.*
[159] Projet de loi du 28 novembre 2000 relative à la criminalité informatique, exposé des motifs, *Doc. Parl.*, Chambre, n° 0213/004, p. 96.

Le faux en informatique requiert une altération de la vérité par la manipulation de données qui « soient dans la vie sociale normale susceptibles de faire preuve, dans une certaine mesure d'un acte ou d'un fait juridique »[160]. Il faut qu'il s'agisse donc d'une altération de la vérité volontaire de données ayant une portée juridique altérée[161].

L'élément moral requis est un dol spécial, bien que l'article 210*bis* du Code pénal ne le mentionne pas expressément[162]. Toutefois, nous pouvons conclure avec certitude qu'en « mentionnant explicitement le faux informatique à l'article 193 du Code pénal, le législateur a clairement marqué son intention d'appliquer à cette nouvelle incrimination les principes compris à l'article 193 » et donc, le dol spécial[163].

Section III. Problèmes de définition et autres incohérences

La création de cette infraction est bénéfique afin de remédier à une violation du principe de légalité qui existait à chaque fois que l'on retenait l'infraction de faux en écriture à des faits ne relevant pas de son champ d'application. Toutefois, il subsiste quelques problèmes relatifs à cette infraction. La terminologie techniquement neutre qui fut utilisée est à notre sens trop vague que pour répondre à l'exigence de clarté de la loi (§1). De plus, le législateur qui souhaitait garder un équilibre entre le faux en informatique et le faux en écriture traditionnel l'a, à notre sens, rompu en créant des différences de traitements sans justification (§2).

§1. Une imprécision déplorable

Dans la loi du 28 novembre 2000, le législateur a choisi d'utiliser une terminologie techniquement neutre[164] afin que la loi ne soit pas trop vite dépassée par l'évolution de la technologie.

Il ne s'agit que de la manipulation de données juridiques pertinente car la simple manipulation de données juridiques n'est pas suffisante. Il faut que ces données aient une valeur juridique telle qu'elles soient généralement jugées comme pouvant faire preuve. L'appréciation de ceci est laissée au juge.
Voy. en ce sens: E. BAEYENS, « Een vals profiel op Facebook : de strafrechter vindt niet leuk », *T. Strafr.*, 2012, vol. 2, pp. 104 à 107; O. LEROUX, « Le faux en informatique », *op. cit.*, p. 513 ; P. DE HERT, « De wet van 28 november inzake informaticacriminaliteit en het materieel strafrecht. Een wet die te laat komt of een wet die er nooit had moeten komen? », *T. Strafr.*, 2001, p. 316.

[160] Cass., 23 décembre 1998, *J.L.M.B.*, 1999, p. 393.

[161] O. LEROUX, « Le faux en informatique », *op. cit.*, p. 512.

[162] J. KERKHOFS en PH. VAN LINTHOUT, « Inleiding tot het materieel en strafprocedureel cyberstrafrecht: uitdagingen voor de advocatuur », *Internet &/@ Recht*, sous la direction de B. DE MEULENAERE, Gent, Larcier, 2013 pp. 5 à 44.

[163] O. LEROUX, « Le faux en informatique », *op. cit.*, p. 514.

[164] J. KERKHOFS et PH. VAN LINDHOUT, « Cybercriminaliteit doorgelicht », *T. Strafr.*, 2010, n°4, p. 181.
Voy. également annexe n° 1, question 2 de la retranscription de l'entretien avec Koen SMETS, inspecteur principal au FCCU, et Marjolein DELPLACE, analyste stratégique du FCCU.

Bien que ceci soit, à priori, utile afin que la loi ne soit pas victime de sa propre précision, il convient malgré tout de pointer du doigt l'absence de définition de deux termes très importants utilisés dans la définition de l'infraction. En effet, les termes « données informatiques » et « système informatique » ne sont pas définis dans la loi[165].

Par contre, l'exposé des motifs de la loi tente d'élaborer une définition mais échoue en définissant chaque terme par rapport à l'autre[166]. En effet, les données sont définies comme étant « les représentations de l'information pouvant être stockées, traitées et transmises par le biais d'un système informatique »[167] et le système informatique y est décrit comme un « système permettant le stockage, le traitement ou la transmission de données »[168].

Ces deux termes sont des termes ayant une importance cruciale pour comprendre la portée de cette infraction. Il aurait été souhaitable que le législateur définisse ces notions sans ambiguïté afin de répondre à l'exigence de légalité substantielle qui requiert une loi pénale claire et précise.

À défaut d'une clarification par le législateur, c'est vers la définition donnée par le Conseil de l'Europe que l'on doit se tourner afin de pouvoir clarifier leur portée.

Selon le Conseil de l'Europe il y a lieu d'entendre par système informatique « tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données ou autres fonctions » et par données informatiques « toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction »[169].

Grâce à ces définitions on peut désormais pallier au manque de clarté de la loi mais il n'en reste pas moins qu'une intervention du législateur belge serait souhaitable afin qu'il n'y ait plus de doute quant à savoir ce qui entre exactement dans le champ d'application de l'infraction. Nous

[165] Projet de loi du 28 novembre 2000 relative à la criminalité informatique, exposé des motifs, *Doc. Parl.*, Chambre, n° 0213/001, p. 12. Voy. également O. LEROUX, « Le faux en informatique », *op. cit.*, p. 512.
[166] CH. MEUNIER, *op. cit.*, pp. 622 à 623.
[167] Projet de loi du 28 novembre 2000 relative à la criminalité informatique, exposé des motifs, *Doc. Parl.*, Chambre, n° 0213/001, p. 12.
[168] Projet de loi du 28 novembre 2000 relative à la criminalité informatique, exposé des motifs, *Doc. Parl.*, Chambre, n° 0213/001, p. 12.
[169] Art. 1 de ladite Convention de Budapest.

éviterions ainsi que les plaideurs tentent d'inclure au sein des cette disposition des faits qui n'y rentreraient pas en vertu de « l'application technologique ou téléologique »[170].

§2. Un problème de discrimination par rapport au faux en écriture

Le problème d'absence de clarté dans les définitions n'est pas la seule difficulté de cette disposition. Un autre problème surgit en ce qu'il existe une discrimination entre le faux en écriture et le faux en informatique.

Le faux en écriture classique opère une distinction dans la gradation des peines. Le faux en écriture authentique et publique est puni plus sévèrement que le faux en écriture[171]. Le faux en informatique, quant à lui, ne se préoccupe pas de cette distinction et punit de la même peine tous les faux en informatique sans avoir égard à la nature de l'écriture[172]. Dès lors, une discrimination existe en ce que « l'auteur d'un faux en écritures authentiques et publiques, par exemple, est passible d'une peine de quinze ans de réclusion, alors que la peine du faux en informatique n'excède pas cinq ans d'emprisonnement »[173].

Une autre discrimination existe aussi entre faux en écriture privée et faux en informatique d' « écriture » privée. Le faux en écriture privée est puni d'une peine criminelle, ce qui n'est pas le cas du faux en informatique d'une « écriture » privée, qui reste sanctionné au moyen d'une peine délictuelle[174].

Selon O. Leroux, ces discriminations sont inconstitutionnelles étant donné que le législateur souhaitait garder un certain équilibre entre les différentes formes de faux et qu'aucun élément ne vient justifier cette différence de traitement[175]. Nous ne pouvons que patienter jusqu'à une éventuelle intervention de la Cour constitutionnelle en la matière…

En conclusion, cette nouvelle incrimination était indispensable pour lutter contre l'impunité et pour mieux respecter le principe de légalité mais elle manque un peu de clarté et de cohérence par rapport à son homologue dans le monde non-numérique. Des améliorations restent à espérer.

---

[170] O. LEROUX, « Le faux en informatique », *op. cit.*, p. 512.
[171] CH. MEUNIER, *op. cit.*, p. 624.
[172] F. DE VILLENFAGNE et S. DUSOLLIER, *op. cit.*, pp. 64 à 65.
[173] CH. MEUNIER, *op. cit.*, p. 624.
[174] CH. MEUNIER, *op. cit.*, p. 624.
[175] O. LEROUX, « Le faux en informatique », *op. cit.*, p. 518 à 519.

Chapitre II. La fraude informatique

La fraude informatique fut introduite dans le Code pénal à l'article 504*quater*. Nous analyserons la définition et le champ d'application de celle-ci (Section I), avant de mettre en exergue les problèmes causés par cette incrimination (Section II).

Section I. Définition et éléments constitutifs

La nécessité d'introduire l'incrimination de « fraude informatique » dans le Code pénal se fit ressentir dès la fin des années '80, principalement pour lutter contre les fraudes de cartes de crédits en tout genre qui ne cessaient d'augmenter et de se diversifier[176].

Ce fut chose faite grâce à la loi du 28 novembre 2000 qui introduit un nouvel article 504*quater* dans le Code pénal réprimant la fraude informatique[177]. Cet article est toujours en vigueur aujourd'hui mais fut légèrement modifié par la loi du 15 mai 2006.

Actuellement l'article 504*quater* du Code pénal prévoit qu'est constitutif d'une fraude informatique le fait pour une personne de chercher à « se procurer, pour lui-même ou pour autrui, avec intention frauduleuse, un avantage économique illégal en introduisant dans un système informatique, en modifiant ou effaçant des données qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation normale des données dans un système informatique »[178]. En d'autres mots, il faut donc la manipulation doleuse de données afin d'obtenir un avantage patrimonial frauduleux.

Il ne faut pas confondre l'infraction de fraude informatique avec l'escroquerie via les nouvelles technologies. L'amalgame est fait par certains auteurs de doctrine[179] alors qu'il s'agit en réalité de deux infractions totalement différentes. Une escroquerie[180] est une infraction ayant pour but de « tromper la confiance d'un tiers, personne physique ou morale, alors que dans le cas de la fraude informatique, il y a tromperie d'une machine »[181].

---

[176] Les principales illustrations ayant menées à la création d'une infraction spécifique de fraude informatique étaient le fait de retirer de l'argent en utilisant une carte de crédit volée, le fait de dépasser illicitement et volontairement avec sa carte de crédit la limite du crédit octroyé… Voy. le projet de loi du 28 novembre 2000 relative à la criminalité informatique, exposé des motifs, *Doc. Parl.*, Chambre, n° 0213/001, p. 14. Voy. également E. BAEYENS, « Informatica en strafrecht : oude griffels – nieuwe leien », *T. Strafr.*, 2007, vol. 6, p. 405.
[177] Code pén., art. 504*quater*.
[178] Code pén., art. 504*quater*.
[179] L'amalgame entre escroquerie et fraude informatique est faite, entre autres, par Christophe Meunier. CH. MEUNIER, *op. cit.*, pp. 626 à 627.
[180] Code pén., art. 496.
[181] I. COLLARD, *op. cit.*, p. 187.

Section II. Problèmes de définition et incohérences

On peut noter que l'infraction de fraude informatique présente de fortes ressemblances avec l'infraction de faux en informatique. Dans de nombreux cas ces deux infractions pourront être retenues ensemble, comme formant une situation de concours[182]. Il est à craindre, cependant, qu'en raison d'une similitude tellement grande, la situation de concours soit appliquée quasi-automatiquement à une infraction qui remplirait les critères d'une de ces infractions. Ceci causerait une aggravation de peine non-justifiée, liée à la similitude des deux infractions[183].

Marjolein Delplace, analyste stratégique au FCCU, affirme d'ailleurs que l'infraction de fraude informatique est presque systématiquement retenue en plus[184]. La raison de la retenue quasi-automatique de cette infraction est le fait qu'elle soit l'infraction de cybercriminalité spécifique la plus lourdement punie.

Il convient donc de se demander s'il était réellement nécessaire de faire deux infractions distinctes vu qu'elles sont la plupart du temps appliquées ensemble et causent une aggravation de peine, due au concours.

Un autre problème de cette infraction est celui d'une violation du principe de légalité dans sa dimension substantielle, à savoir que la loi n'est pas claire et précise. En effet, comme abordé précédemment[185], les termes essentiels « système informatique » et « données » ne sont pas définis par le législateur et comportent des contours flous, de sorte qu'il n'est pas toujours clair de savoir quels comportements entrent ou non dans le champ d'application de l'incrimination.

Chapitre III. Les infractions contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données qui sont stockées, traitées ou transmises par ces systèmes

Les infractions contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données qui y sont stockées, traitées ou transmises par ces systèmes, on

[182] CH. MEUNIER, *op. cit.*, p. 627 ; O. LEROUX, « Arnaques, fraudes et escroqueries sur internet : moyens concrets d'investigation. Point sur l'affaire dite *Yahoo !* à la suite du second arrêt de la Cour de cassation », *J.T.*, 2012, p. 840.
[183] O. Leroux craint que le concours idéal soit retenu de façon quasi-automatique entre le faux en informatique et d'autres infractions ce qui aura des conséquences dramatiques en termes de peines.
[184] Voy. annexe n° 1, question 5 de la retranscription de l'interview avec l'inspecteur Koen SMETS et Marjolein DELPLACE.
[185] Voy. pour plus de précisions Partie II – Titre II – Chapitre I – Section III - §1.

retrouve d'une part l'accès non-autorisé à un système informatique (Section I) et d'autre part le sabotage informatique (Section II).

Nous analyserons en premier lieu ces deux types d'infractions en tant que telles, avant de poser un regard critique sur les problèmes causés par celles-ci (Section III).

Section I. L'accès non autorisé à un système informatique

L'accès non-autorisé à un système informatique est le fait d'accéder sans autorisation au système informatique d'un tiers, à l'insu de celui-ci. Cette infraction est mieux connue sous sa dénomination anglaise : le *hacking*.

Le *hacking* existe sous diverses formes et est incriminé par l'article 550*bis* du Code pénal. Cet article fut également introduit par la loi du 28 novembre 2000 et fut très légèrement modifié par la suite, six ans plus tard, par la loi du 15 mai 2006.

Il existe deux formes de *hacking*. Le *hacking* externe prévu au §1 de l'article 550*bis* du Code pénal incrimine le comportement de « celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient » [186] sans en avoir reçu l'autorisation. Le *hacking* interne, par contre, prévu au §2 de l'article 550*bis* du Code pénal, incrimine le « fait d'outrepasser son pouvoir d'accès à un système informatique, avec intention frauduleuse ou dans le but de nuire »[187].

Section II. Le sabotage informatique

L'infraction de sabotage informatique fut introduit afin de réprimer tous les comportements qui portent atteinte à l'intégrité d'un système informatique « en l'endommageant, en entravant le fonctionnement correct ou en affectant les données qu'il contient, stocke ou transmet »[188]. Il s'agit donc de réprimer l'auteur d'un fait qui « modifie ou efface des données, ou qui modifie par tout moyen technologique l'utilisation normale de données dans un système informatique »[189].

Tout comme les infractions précédemment évoquées, l'infraction de sabotage informatique fut introduit en droit belge par la loi du 28 novembre 2000 et modifié par la loi du 15 mai 2006.

[186] Code pén., 550*bis* §1.
[187] I. COLLARD, *op. cit.*, p. 188.
[188] CH. MEUNIER, *op. cit.*, p. 646.
[189] Code pén., art. 550*ter*.

Section III. Les problèmes de définition et de cohérences

Une fois de plus, pour cette catégorie d'infractions, il y a lieu de pointer du doigt le manque de clarté et de précision des termes utilisés[190].

De plus, dans le délit de *hacking*, il convient d'épingler un risque de pénalisation excessive. En effet, tout accès ou maintien non autorisé se trouve pénalisé, sans qu'une intention frauduleuse ou que la transgression d'un système de sécurité ne soit requise.

Bien que le Conseil d'État ait émis des craintes quant au risque d'une pénalisation excessive, le législateur estime que la protection de l'intégrité du système informatique surpasse les autres intérêts juridiques.

L'inspecteur principal du FCCU, Koen Smets, souligne également que ceci est une aberration de la législation pénale belge[191].

Plusieurs auteurs, comme F. de Villenfagne et S. Dussolier nous font remarquer que la définition actuelle a pour conséquence que, par exemple, « tout expert en sécurité informatique qui tente de déverrouiller les dispositifs de protection afin de vérifier la fiabilité et l'efficacité »[192] de ceux-ci, se rendent coupable de *hacking* et s'exposent à des poursuites pénales.

De plus, la simple visite de curiosité dans un système informatique non-protégé, auquel l'accès n'impliquerait donc aucun « cassage » de dispositifs de sécurité, constitue désormais une infraction[193]. Toute personne utilisant un réseau Wi-Fi non protégé se rend coupable de *hacking*, souvent sans savoir que le fait de se connecter à ce réseau est constitutif d'une infraction.

L'intention de nuire n'est pas un élément constitutif de l'infraction, sinon une circonstance aggravante[194].

Une affaire interpellant en la matière fut jugée en 2004 par le tribunal correctionnel d'Hasselt[195]. Un gestionnaire de réseau s'était, par hasard, rendu compte que le système informatique de la

---

[190] Nous ne reviendrons pas en détail sur cette problématique qui fut abordée en profondeur dans Partie II – Titre II – Chapitre I – Section III - §1.
[191] Voy. annexe n° 1, question 12 de la retranscription de l'interview avec l'inspecteur Koen SMETS et Marjolein DELPLACE.
[192] F. DE VILLENFAGNE et S. DUSOLLIER, *op. cit.*, p. 69.
[193] J. KERKHOFS en PH. VAN LINTHOUT, « Inleiding tot het materieel en strafprocedureel cyberstrafrecht: uitdagingen voor de advocatuur », *op. cit.*, p. 15.
[194] *Ibidem*
[195] Corr. Hasselt, 21 janvier 2004, *Computerr.*, 2004, liv. 3, p. 130.

banque DEXIA ne disposait pas de système de sécurité. Suite à cela, il était possible pour toute personne, ayant quelques connaissances en informatique, de rentrer dans ce système informatique et de modifier des données telles que des numéros de compte. Ceci aurait pu occasionner des conséquences dramatiques. Cet homme, n'ayant aucune mauvaise intention, a prévenu de façon subtile la banque DEXIA de sa faille de sécurité en entrant dans le système et en y laissant une trace de son passage. Malgré cette trace, la banque ne modifia pas son système de sécurité. Le *hacker* décida alors d'alerter la banque DEXIA par *e-mail* afin qu'elle puisse remédier à ce problème de sécurité. Bien que le *hacker* était animé de bonnes intentions, la banque décida de porter plainte contre lui suite à son *e-mail* dans lequel il signalait qu'il était possible de s'introduire dans leur système comme il l'avait lui-même fait.

Etant donné qu'aucune intention frauduleuse n'est requise pour que l'infraction d'introduction dans un système informatique soit réalisée, le *hacker* fut poursuivi puis déclaré coupable par le tribunal, bien qu'au final il bénéficia d'un jugement indulgent.

Deux solutions possibles s'offrent à ce problème de pénalisation excessive.

La première solution serait de suivre la démarche des Pays-Bas afin de rendre l'infraction de *hacking* punissable uniquement lorsqu'il y a transgression d'un système de sécurité[196]. Dès lors, les personnes ne faisant pas l'effort de sécuriser leur système, ne pourraient pas ensuite se retourner contre une personne curieuse qui y serait entrée.

Bien qu'étant une solution partielle, cette solution ne parait cependant pas idéale. Comme le signale, S. Dussolier, chercheuse au centre de recherches informatiques et de droit des F.U.N.D.P. Namur, « l'explication des mesures de sécurité et de leur contournement sera nécessaire à l'établissement de l'infraction. […] Les plaignants […] seront peu enclins à produire de tels éléments, qui seraient préjudiciables pour leur sécurité future »[197].

Une autre solution, probablement meilleure, serait d'imposer un dol spécial comme élément constitutif de l'infraction. Néanmoins, cette hypothèse a été clairement rejetée par le législateur qui estime que la protection du système informatique est l'intérêt suprême en la matière[198]. Toutefois, rien n'empêcherait un retour de la part de celui-ci sur sa décision initiale.

---

[196] Au Pays-Bas l'infraction de *hacking* n'est possible que pour les systèmes informatiques qui sont protégés par un système de sécurité. Code pén. néerlandais, art. 138a.
[197] F. DE VILLENFAGNE et S. DUSOLLIER, *op. cit.*, p. 70.
[198] Projet de loi du 28 novembre 2000 relative à la criminalité informatique, exposé des motifs, *Doc. Parl.*, Chambre, n° 0213/001, p. 17.

EN GUISE DE CONCLUSION, QUELQUES RÉFLEXIONS SUR LE DROIT PÉNAL MATÉRIEL DU CYBERMONDE

Comme évoqué dans les chapitres précédents, le droit matériel de la cybercriminalité est un droit qui s'articule en deux parties : une partie de cybercriminalité non-spécifique et une partie de cybercriminalité nouvelle et spécifique.

A l'issue de l'analyse des infractions du cybermonde et de la mise en exergue des problèmes en la matière, il convient de se poser deux questions.

Premièrement, il convient de se demander s'il faudrait créer plus d'infractions de cybercriminalité spécifique, ou si le droit matériel tel qu'il existe aujourd'hui est suffisant pour pénaliser tous les comportements non désirables réalisés dans le monde des NTIC.

Ensuite, il faut se poser la question de savoir si l'on peut continuer à appliquer les principes qui régissent le droit matériel traditionnel aux infractions du cybermonde, ou si l'on doit créer une section du Code pénal uniquement pour les cyberdélits, avec d'autres principes qui s'y appliquent.

Première réflexion : Le droit pénal matériel, est-il suffisant ?

En ce qui concerne la première question, la Belgique fait actuellement partie des bons élèves en la matière. Les comportements qu'il n'était pas possible de punir à travers les infractions traditionnelles ont bénéficié d'un nouvel encadrement juridique grâce à la loi du 28 novembre 2000. Le législateur s'y est pris tard, certes, mais l'encadrement juridique actuel est en grande partie satisfaisant.

En ce qui concerne la cybercriminalité non-spécifique, il est vrai que de nombreux comportements sont actuellement encore punis au moyen de l'infraction traditionnelle telle que l'escroquerie sur Internet, les jeux de hasards sur Internet, la pédopornographie sur Internet… Toutefois, il s'agit souvent de la criminalité informatique qui utilise les NTIC comme moyen, et non comme objet de l'infraction. Il n'est, dès lors, dans de nombreux cas, pas nécessaire d'adapter l'infraction traditionnelle car l'infraction, bien que commise dans le cybermonde, entre sans aucun problème dans le champ d'application de l'infraction traditionnelle.

Toutefois, nous avons relevé le cas du « vol » de données qui est un problème qu'il convient de résoudre. En effet, actuellement le cas de « vol » de données est puni de diverses façons : soit

par l'infraction de vol dans le cadre d'un *hacking*, soit par l'infraction traditionnelle, soit au moyen d'autres législations telles que la législation sur les droits d'auteurs ou les articles relatifs à l'abus de confiance.

Pour la majorité des autres infractions traditionnelles, elles sont, à l'heure d'aujourd'hui, encore aptes à inclure dans leur champ d'application leur « équivalent » numérique.

Toutefois, il est important que le législateur et des experts en informatique et criminalité informatique tel que le FCCU restent attentifs afin de vérifier qu'aucun comportement nouveau ne surgisse pour lequel il n'existe pas d'incrimination adéquate. La Belgique ne peut pas prendre le risque d'une impunité pour des comportements qui devraient être punissables mais qui ne peuvent pas être réprimés à cause d'un vide juridique.

En ce qui concerne la cybercriminalité spécifique, l'inspecteur principal du FCCU, Koen Smets, estime que tous les comportements répréhensibles sur Internet peuvent actuellement être inclus dans les dispositions dont on dispose en Belgique[199]. En effet, le législateur belge a opté pour une terminologie techniquement neutre qui, selon l'inspecteur Koen Smets, permet d'être interprétée de telle façon qu'il soit possible de faire rentrer tous les comportements répréhensibles d'Internet et des nouvelles technologies dans son champ d'application.

Jugé par le FCCU comme une bonne chose, il nous parait néanmoins critiquable d'avoir une législation qui manque à ce point de clarté qu'elle puisse être « tordue » dans tous les sens afin de faire entrer tous les comportements répréhensibles qui se produisent au moyen des NTIC ou qui ont celles-ci comme cible dans un arsenal juridique comportant seulement quatre infractions. Une terminologie techniquement neutre est effectivement un impératif afin de pouvoir survivre face aux différentes évolutions du monde numérique. Cependant, cette terminologie ne doit pas violer le principe de légalité en son sens substantiel en s'affranchissant de définitions et d'un minimum de clarté.

En conclusion, on peut donc dire que l'arsenal législatif belge est relativement adéquat en ce qu'il permet d'encadrer la toute grande majorité des comportements nuisibles commis sur Internet. Toutefois, une mise à jour est nécessaire car la réalité virtuelle d'il y a quinze ans, n'est plus celle d'aujourd'hui. De plus, ceci permettrait de mieux répondre à l'exigence de légalité des infractions en matière pénale.

[199] Voy. annexe n°1, question 2 de la retranscription de l'entretien effectué avec Koen SMETS et Marjolein DELPLACE, membres du FCCU.

Deuxième réflexion. Un volet spécifique pour le droit pénal matériel du cybermonde est-il souhaitable ?

Certains pourraient être amenés à penser qu'en raison de la spécificité même du cybermonde, il serait nécessaire de faire un volet à part pour le droit matériel du cybermonde. Ce volet matériel serait régi par ses propres principes et s'affranchirait du principe de légalité[200].

Il est vrai que dans les nouvelles infractions de cybercriminalité, le principe de légalité se trouve violé à plusieurs reprises à cause du manque de précision des nouvelles dispositions. De plus, dans la cybercriminalité non-spécifique, bien souvent, on étend également le champ d'application matériel d'une infraction traditionnelle, plus loin que ce qui était l'intention du législateur.

Pourtant, selon nous il n'est pas souhaitable d'envisager une section propre à la cybercriminalité au sein du droit pénal matériel qui s'affranchirait – ou assouplirait – le principe de légalité. En effet, le principe de légalité est une pierre angulaire de notre droit pénal et constitue une garantie contre l'arbitraire. La solution, selon nous, consisterait simplement en une obligation pour le législateur de revoir sa copie concernant certaines infractions afin de répondre de façon plus adéquate à l'exigence de clarté.

Il est inadmissible que des notions clés telles que « données » ou « système informatique » ne soient pas définies dans la loi et que des infractions soient définies de façons à ce point large qu'il soit possible d'y faire entrer tous les nouveaux comportements indésirables du cybermonde, comme l'avoue l'inspecteur principal du FCCU, Koen Smets.

La nécessité de définir certaines notions-clés se fait pressante mais il est utopique de penser que le législateur pourrait clarifier toutes les notions utilisées dans ces nouvelles incriminations. L'utilisation de notions larges est souvent l'intention même du législateur afin de pouvoir intégrer des comportements qui, certes, aujourd'hui n'existent pas encore mais qui surgiront demain dans le cyberespace. Ainsi le législateur essaye d'éviter qu'une modification de la loi soit nécessaire à chaque fois qu'un nouveau comportement fait surface.

Nous sommes conscients de cette difficulté et acceptons le choix d'une terminologie techniquement neutre mais des efforts de précisions sont néanmoins à prôner.

---

[200] La remise en cause du principe de légalité fut opérée par certains états. Nous pouvons retenir à titre d'exemple le Code pénal soviétique de 1921 qui s'est totalement affranchi de ce principe. Plus d'informations disponible dans : J. BELLON, *Droit pénal soviétique et droit pénal occidental,* Paris, Editions de Navarre, p. 1961 cité dans F. TULKENS e.a., *op. cit.*, p. 230.

PARTIE III – LE DROIT DE LA PROCÉDURE PÉNALE

Le cybermonde est un espace « virtuel, immatériel, en tout cas sans frontières, mondialisé et universel »[201]. Tout y est plus rapide que dans le monde réel, les frontières n'existent pas, l'anonymat est la règle et tout est immatériel.

De nombreux problèmes furent pointés du doigt, liés aux caractéristiques-mêmes du cybermonde et ont amené le législateur à réagir. Tout comme pour le droit pénal matériel, les principales adaptations furent réalisées par la loi du 28 novembre 2000 qui vint modifier le Code d'instruction criminelle et la dite loi Belgacom[202]. Cette loi opéra une mise à jour de la procédure pénale pour l'adapter à la réalité de la société de l'information, mais elle ne perpétra pas de révolution profonde des mécanismes procéduraux[203].

Outre l'adaptation législative, d'autres initiatives furent mises en place afin de rechercher et de poursuivre plus efficacement la cybercriminalité, telles que l'optimisation des entités de recherche, comme le *Federal Computer Crime Unit*.

La loi belge du 28 novembre 2000 précéda de peu l'entrée en vigueur de la Convention de Budapest et il y lieu de croire que le législateur belge se serait laissé influencer par la création de celle-ci afin de munir la Belgique, dès le départ, d'une législation qui serait conforme à la Convention[204]. De nombreuses similitudes sont à noter entre ces deux textes, toutefois les infractions prévues par le législateur belge vont plus loin que celles prévues par la Convention.

Dans les prochains chapitres, nous analyserons la législation en matière de procédure pénale relative au cybermonde et pointerons du doigt les incohérences et difficultés de celle-ci (Chapitre I). Ensuite, nous nous pencherons sur les autorités compétentes en matière de recherche, en nous attardant particulièrement sur le FCCU (Chapitre II). Nous procéderons également à une analyse à propos de l'efficacité des poursuites pour les infractions informatiques (Chapitre III). À travers l'analyse de la législation et des mécanismes de recherche et de poursuite, nous pourrons ensuite tirer des conclusions sur l'efficacité du droit de la procédure pénale en matière de cybercriminalité.

---

[201] J. FRANCILLON, *op. cit.*, p. 1.
[202] CH. MEUNIER, *op. cit.*, p. 651.
[203] Projet de loi du 28 novembre 2000 relative à la criminalité informatique, exposé des motifs, *Doc. Parl.*, Chambre, n° 0213/001, p. 9. Voy. également KEUSTERMANS, J. et DE MAERE, T., *op. cit.*, p. 567.
[204] K. VERHAEGE, *op. cit.*, p. 94.

Chapitre I. Les nouveaux mécanismes de procédure pénale

La conservation de données (Section I), la saisie des données informatiques (Section II), la recherche sur les réseaux (Section III), l'injonction de produire (Section IV) et l'obligation de coopération (Section V) furent les principales modifications intervenues dans la législation belge pour adapter celle-ci à un environnement virtuel.

Section I. La conservation des données

Un premier problème de procédure pénale présent dans le monde virtuel était la précarité des informations. Les données des systèmes informatiques étaient habituellement effacées après quelques heures, voire même jamais conservées. En raison de ce caractère volatile, il était très difficile de rechercher des preuves car, passé un bref délai, ces informations n'étaient plus accessibles.

Très vite, une obligation de conservation de données fut dès lors mise en place en Belgique pour tenter de remédier à cette problématique. Cette obligation a connu de nombreux rebondissements, certains très récemment[205].

Le processus de rédaction de la Convention de Budapest était déjà enclenché au moment où le législateur belge créa la première obligation de conservation de données. Bien que le régime belge s'inspira du régime qui allait devenir celui de la Convention, notre législateur fut néanmoins beaucoup plus sévère[206].

Là où les articles 16 et 17 de la Convention de Budapest instauraient une obligation de conservation pour une durée de 90 jours, la Belgique imposait une durée beaucoup plus longue de douze mois au minimum[207].

Jusqu'alors, il s'agissait d'une conservation limitée à certaines données spécifiquement énumérées[208]. Quelques années plus tard, en 2006, une directive européenne[209] fut adoptée qui

[205] Au cours de la rédaction de ce mémoire, le rebondissement le plus significatif eut lieu et mena à l'abolition de toute obligation de conservation/rétention de données.
[206] K. VERHAEGE, *op. cit.*, p. 94.
[207] Ancien art. 109*ter* E de la loi du 21 mars 1999 portant réforme à certaines entreprises publiques économiques, *M.B.*, 27 mars 1991. Cet article fut abrogé en 2005 par l'article 55 de la loi du 13 juin 2005 relative aux communications électroniques, *M.B.*, 20 juin 2005. Cette loi mît en place un dispositif similaire dans son article 126 qui prévoit également une durée de conservation de douze mois minimum.
[208] Art. 126 de la loi du 13 juin 2005 relative aux communications électroniques, *M.B.*, 20 juin 2005.
[209] Directive (CE) n° 2006/24 du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au

élargit sensiblement les données qui devaient être conservées[210]. Cette directive fut transposée, très tardivement en Belgique par la loi du 30 juillet 2013[211].

Tant la directive que la loi belge firent couler beaucoup d'encre, car si l'obligation de conservation élargie facilitait considérablement le travail des enquêteurs dans la recherche de preuves et l'identification des auteurs, elle causait néanmoins des cauchemars aux défenseurs des libertés fondamentales. Le caractère généralisé de la conservation, sans la limiter aux données strictement nécessaires, et les risques d'ingérences furent l'objet de vives critiques. À l'heure où la protection de la vie privée est au centre des préoccupations de notre société, la conservation de données ne plaisait pas.

Suite à tant de critiques, des questions préjudicielles sur la validité de la directive furent présentées devant la Cour de justice de l'Union Européenne. Dans les affaires jointes C-293/12 et C-594/12[212] la Cour de Justice de l'Union Européenne déclara la directive sur la rétention des données invalide en raison de sa non-proportionnalité[213].

Cette directive étant dès lors réputée n'avoir jamais existé, la suite logique des événements mena récemment à un recours en annulation devant la Cour constitutionnelle belge. La saga prit fin le 11 juin 2015 et mena à l'annulation de la loi du 30 juillet 2013[214]. L'article 126 de la loi du 13 juin 2005 relative aux communications électronique est dès lors à nouveau d'application en la matière, mais consiste en une rétention de données beaucoup plus limitée.

Bien que les défenseurs des droits de l'homme soient ravis de voir cette loi annulée, le Ministre de la Justice, Koen Geens, ne s'en réjouit que moyennement. Avouant qu'il s'agit d'une victoire pour les droits de l'homme, il espère malgré tout qu'une nouvelle loi ou directive européenne verra le jour rapidement. Sans la possibilité de conserver les données comme avant, il craint une grande perte d'efficacité dans la recherche des infractions du cybermonde.

public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, *J.O.U.E.*, L.105/54, 13 avril 2006.

[210] C. CONINGS et F. VERBRUGGEN, « Grondwettelijk Hof plaatst reparateurs dataretentiewet voor moeilijke opdracht », *Juristenkrant*, 2015, n° 312, p. 1.

[211] Loi du 30 juillet 2013 portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90*decies* du Code d'instruction criminelle, *M.B.*, 23 août 2013.

[212] C.J.U.E. (grande chambre), 8 avril 2014, (Digital Rights Ireland Ltd, Kärntner Landesregierung, e.a.), C-293/12 et C-594/12, disponible sur : http://curia.europa.eu/.

[213] Le §69 de la décision de la C.J.U.E. estime que : « Eu égard à l'ensemble des considérations qui précèdent, il convient de considérer que, en adoptant la directive 2006/24, le législateur de l'Union a excédé les limites qu'impose le respect du principe de proportionnalité au regard des articles 7, 8 et 52, paragraphe 1, de la Charte ».

[214] C.C., 11 juin 2015, n° 84/2015.

Koen Smets, inspecteur principal au FCCU, va plus loin en disant que, dans la situation actuelle, si la rétention et conservation de données restent limitées le FCCU et les RCCU[215] se retrouvent dans une situation comparable à celle d'un chômage technique en ce sens qu'ils ne pourront plus enquêter efficacement[216].

Bien entendu, le FCCU dispose d'autres moyens d'enquête mais l'inspecteur estime que le seul moyen pouvant compenser la rétention de données est l'augmentation drastique du nombre de perquisitions, de saisies et de prises de connaissance de télécommunications privées bien que ces mesures constituent selon lui une atteinte encore plus grave aux libertés individuelles[217].

Nous ne pouvons que nous joindre à l'avis du FCCU et du Ministre de la Justice à propos de cette thématique et espérer que notre législateur, ou mieux une convention internationale, trouvera une solution afin de permettre une rétention des données sans violer les droits fondamentaux[218].

Le droit à la vie privée n'est pas un droit absolu et il convient de mettre dans la balance également d'autres intérêts, tels que l'efficacité de la recherche des infractions. Comme le souligne l'inspecteur principal du FCCU, Koen Smets, ce n'est pas parce que les données sont accessibles aux autorités de recherche, que la police contrôle nécessairement l'ensemble des comportements des citoyens[219]. En effet, l'accès aux données conservées se ferait moyennant certaines conditions et le droit à la vie privée serait encore garanti.

Section II. La saisie de données et la recherche sur les systèmes informatiques pour pallier les problèmes d'immatérialité

Étant donné l'immatérialité des données sur Internet, les procédures judiciaires traditionnelles sont souvent inadéquates et non-transposables à des délits commis dans le cybermonde[220]. La procédure de saisie en était un exemple parfait, avant l'intervention législative de 2000.

---

[215] *Regional Computer Crime Units*

[216] Voy. annexe n° 1, question 11 de la retranscription de l'entretien avec l'inspecteur Koen SMETS et l'analyste stratégique Marjolein DELPLACE.

[217] Voy. annexe n° 1, question 11 de la retranscription de l'entretien avec l'inspecteur Koen SMETS et l'analyste stratégique Marjolein DELPLACE.

[218] Le 4 août 2015, le quotidien Le Soir fit part d'un avant-projet de loi rédigé en un mois à peine afin de réagir à l'annulation de la loi du 30 juillet 2013. Cet avant-projet de loi souhaite instaurer une conservation de données en répondant aux critiques de la Cour constitutionnelle. J.-F. HENROTTE, qui était responsable du recours en annulation de la loi du 30 juillet 2013, s'est déjà manifesté en disant qu'il attaquerait la loi si l'avant-projet se concrétiserait. J.-F. MUNSTER, « L'accès à nos données sera mieux encadré », Le Soir, mardi 4 août 2015. Voy. annexe n° 10 pour l'article complet.

[219] Voy. annexe n° 1, question 11 de la retranscription de l'entretien avec l'inspecteur Koen SMETS et l'analyste stratégique Marjolein DELPLACE.

[220] F. DE VILLENFAGNE et S. DUSOLLIER, *op. cit.*, pp. 72 à 73.

Avant la loi de 2000, lorsque les autorités compétentes souhaitaient prendre connaissance de données informatiques stockées dans des d'ordinateurs, afin de les utiliser comme pièce à conviction, le seul recours était le recours à la saisie de tout le matériel informatique vu qu'il était impossible de saisir les données en tant que telles[221].

Ceci était une mesure particulièrement lourde et qui pouvait mener à des situations dramatiques dans lesquelles des entreprises allaient droit à la faillite.

F. de Villenfagne et S. Dussolier citent le cas hypothétique d'une entreprise de graphisme dont les ordinateurs feraient l'objet d'une saisie suite à un soupçon de violation de propriété intellectuelle[222]. Pour le simple fait d'être soupçonnée d'avoir utilisé sans autorisation l'œuvre d'autrui, cette entreprise se verrait privée de tout son matériel informatique et serait dans l'incapacité complète de continuer à travailler durant toute la durée de l'enquête.

Le recours à cette mesure était relativement lourd mais était appliqué vu que c'était l'unique solution applicable.

Cette solution, en plus d'être lourde et d'avoir des effets disproportionnés, ne permettait pas non plus d'être totalement efficace. De nombreuses entreprises possèdent des systèmes informatiques complexes avec des parties stockées dans d'autres endroits, voire même à l'étranger, et il n'est pas aisé d'aller saisir tout le matériel informatique[223]. Dans le cas de grosses multinationales, ceci paraît tout simplement impossible[224].

La nécessité de trouver une solution à ces problèmes se faisait sentir. Ce fut chose faite avec la loi du 28 novembre 2000 qui augmenta les possibilités des autorités de recherche en prévoyant la saisie de données immatérielles dans l'article 39*bis* dans le Code d'instruction criminelle.

Bien entendu, il est toujours possible d'avoir recours à la saisie traditionnelle et saisir tout le matériel informatique mais cette solution n'est plus que très rarement appliquée car l'article 39*bis* du Code d'instruction criminelle prévoit d'autres solutions moins lourdes telles que le fait de copier ou de rendre inaccessible – voir même d'effacer – des données afin de servir de preuve.

---

[221] En effet, la saisie traditionnelle ne s'applique qu'à des choses matérielles selon l'art. 35 du C.i.cr. Voy. en ce sens : F. DE VILLENFAGNE et S. DUSOLLIER, *op. cit.*, pp. 72 à 73.
[222] F. DE VILLENFAGNE et S. DUSOLLIER, *op. cit.*, pp. 72 à 73.
[223] *Ibidem*
[224] *Ibidem*

La copie des données informatique est préférée aux deux autres possibilités[225]. Si l'utilisation des données ne présente pas de risque d'affecter le travail de la collecte de preuve, ni d'affecter l'intégrité des preuves déjà collectées, le législateur prévoit la possibilité de les copier en les laissant accessibles[226]. C'est seulement dans les cas où la copie ne serait pas possible matériellement ou si le risque de déperdition de preuve est trop grand, que les autorités de recherche peuvent bloquer l'accès aux données afin de préserver leur intégrité pour les recherches pénales ou les supprimer[227].

La suppression de données est rare et n'a lieu que dans les cas où « les données forment l'objet de l'infraction ou ont été produites par l'infraction et si elles sont contraires à l'ordre public ou aux bonnes mœurs ou constituent un danger pour l'intégrité des systèmes informatiques ou pour des données, stockées, traitées ou transmises par le biais de tels systèmes »[228].

L'instauration de cet article facilita grandement le travail des équipes de recherche et permit d'éviter la disproportion dans les enquêtes. Toutefois, quelques remarques peuvent lui être adressées.

L'imprécision est une fois de plus présente dans cet article. À plusieurs reprises le législateur a recours à la notion de « moyens techniques appropriés ». Ces termes furent choisis par soucis d'utiliser une terminologie techniquement neutre et capable de suivre l'évolution technologique mais ils ont des contours flous. Cette imprécision crée un doute quant à savoir exactement comment la saisie de données informatiques doit avoir lieu[229]. Kerkhofs et Van Lindhout estime qu'une définition est nécessaire et que l'on pourrait se baser sur la législation de nos voisins en la matière afin de remédier à cette imprécision. Sans une définition claire et précise, le doute persistera.

Une autre critique pouvant être faite par rapport à cet article est qu'il arrive que les données formant l'objet de la saisie se situent dans le système informatique d'un tiers, le « responsable du système informatique »[230].

Ce responsable du système informatique est informé de la saisie des données et aura la possibilité de demander la mainlevée de celle-ci. Toutefois, le terme « responsable du système informatique » ne vise que les personnes qui disposent formellement du contrôle du système

[225] C.i.cr., art. 39*bis*.
[226] J. KERKHOFS et PH. VAN LINDHOUT, « Cybercriminaliteit doorgelicht », *op. cit.*, p. 190.
[227] *Ibidem*
[228] C.i.cr., art. 39*bis*, §3.
[229] J. KERKHOFS et PH. VAN LINDHOUT, « Cybercriminaliteit doorgelicht », *op. cit.*, p. 191.
[230] F. DE VILLENFAGNE et S. DUSOLLIER, *op. cit.*, p. 74.

informatique, sans se soucier de la personne qui dispose du contrôle réel[231]. Ainsi l'article permettra aux fournisseurs d'hébergement de pages web sur un serveur de contester la saisie, alors qu'il ne le permet pas à la personne responsable des pages Web dont l'accès aura été rendu indisponible[232].

Cette injustice fut relevée par le Conseil d'état qui a suggéré d'inclure non seulement les personnes disposant du contrôle formel, mais aussi du contrôle réel du système informatique objet de la perquisition[233]. À l'heure d'aujourd'hui, ce n'est malheureusement pas encore solutionné.

Cependant, dans son ensemble cet article est efficace et a permis aux autorités de recherche d'amoindrir les coûts de la recherche et de rendre la procédure moins lourde.

Section III. La recherche sur les systèmes informatiques

Afin de remédier aux nombreuses perquisitions dans différents lieux et à la saisie de tout le matériel informatique rencontré dans ces divers lieux, le législateur belge instaura un mécanisme de recherche de preuves sur les systèmes informatiques. Ce système se rapproche de l'institution de la perquisition, mais reste une institution singulière[234] qui permet d'accroître l'efficacité des recherches tant sur le plan national (§1) qu'international (§2).

§1. En Belgique

La recherche sur les systèmes informatiques est une institution particulière qui se rapproche très fortement de la perquisition. Certains auteurs assimilent d'ailleurs – à tort – les deux institutions[235]. En réalité, il s'agit d'une institution singulière qui prend place dans le cadre d'une perquisition physique.

Alors qu'aucune disposition du Code d'instruction criminelle ne règle spécifiquement la recherche sur les systèmes informatiques, l'article 88*ter* du Code d'instruction criminelle quant à lui fait référence à la possible extension lors d'une telle recherche[236]. Cette extension consiste,

---

[231] *Ibidem*
[232] *Ibidem*
[233] *Ibidem*
[234] C. FORGET, « La collecte de preuves informatiques en matière pénale », *Pas de droit sans technologie*, Bruxelles, Larcier, 2015, p. 253.
[235] CH. MEUNIER assimile à tort la recherche sur les systèmes informatiques à une perquisition. Il écrit « il nous paraît cohérent d'assimiler la recherche informatique à une perquisition » dans CH. MEUNIER, *op. cit.*, pp. 663. Ceci est erroné, et l'ensemble de la doctrine semble avoir admis aujourd'hui qu'il s'agit d'une institution singulière, distincte de la perquisition physique.
[236] C. FORGET, *op. cit.*, p. 254.

pour les autorités de recherches qui ont l'autorisation de rechercher au sein d'un système informatique, d'étendre sous certaines conditions leur recherche aux parties de ce système informatique complexe qui se situe dans un autre lieu[237]. Cet article requiert qu'une préalable autorisation de recherche au sein d'un système informatique existe. Certains auteurs estiment que ce préalable est rempli par l'existence même d'un mandat de perquisition tandis que d'autres estiment que l'autorisation de recherche du système informatique doit être inscrite spécifiquement dans celui-ci[238].

Une fois ce préalable rempli, l'article *88ter* du Code d'instruction criminelle prévoit que l'extension peut avoir lieu lorsqu'elle est nécessaire à la manifestation de la vérité et que l'utilisation d'autres mesures serait disproportionnée ou causerait un risque de déperdition d'éléments de preuves.

Cette extension n'est pas sans limite. Seuls les systèmes informatiques, ou parties de tels systèmes auxquels les personnes autorisées à utiliser le système informatique qui fait l'objet de la mesure ont spécifiquement accès, peuvent être fouillés par les autorités de recherche[239].

Les données qui seraient utiles à l'enquête pourront faire l'objet de mesures de saisies de données, évoquées précédemment.

Cet article est extrêmement utile, mais nous ne pouvons que relever le manque de clarté, une fois de plus, du législateur[240]. Une intervention législative devrait avoir lieu pour, entre autres, préciser dans quel cas la simple recherche sur le réseau – ce préalable nécessaire à l'application de l'article 88*ter* C.i.cr. – serait possible.

§2. À l'étranger

Alors que l'article 19 de la Convention de Budapest ne prévoit la recherche sur les systèmes informatiques qu'à l'intérieur des frontières d'un état, la Belgique va plus loin et permet une recherche également sur les parties du réseau informatique situées à l'étranger dans le troisième paragraphe de l'article 88*ter* du Code d'instruction criminelle.

Afin de ne pas léser la souveraineté des états dans lesquels la recherche est effectuée, les possibilités des autorités compétentes sont plus limitées que sur un plan national. En effet, il

[237] *Ibidem*
[238] KERKHOFS, J. et VAN LINTHOUT, PH., « Cybercriminaliteit doorgelicht », *op. cit.*, p. 198.
[239] C. FORGET, *op. cit.*, p. 254.
[240] INCALZA, T., « Strafonderzoek in het digitale tijdperk : zoeking en inbeslagneming », *Jura Falc.*, 2010-2011, vol. 2, p. 381.

leur est uniquement autorisé d'effectuer des copies des données[241]. Cette copie de donnée est de surcroît uniquement permise lorsque la découverte de l'élément international se fait après le début de l'enquête[242]. Le fait de rendre inaccessibles certaines données ou parties d'un système informatique afin d'y effectuer des recherches ou d'effacer certaines données, n'est pas admis lorsque le cyberdélit comporte une dimension internationale.

Le juge d'instruction qui effectue des copies de données dans un système informatique totalement ou partiellement situé à l'étranger est tenu d'en informer le Ministre de la Justice qui à son tour se mettra en contact avec les autorités compétentes dans l'état étranger[243]. Aucune autorisation n'est requise[244]. L'information de l'autorité compétente dans l'état étranger est suffisante. Dès lors, vu le caractère intrusif dans la souveraineté d'un état voisin, cette méthode d'utilisation doit rester exceptionnelle. En effet, d'autres moyens, moins intrusifs, existent pour mener à bien des enquêtes dans une situation à caractère international et doivent être préférés[245]. Ce n'est que dans des cas d'extrême nécessité que la méthode de l'article 88*ter* du Code d'instruction criminelle pourra être utilisée.

Cette atteinte à la souveraineté d'un autre état nous semble critiquable tant qu'aucune convention internationale n'intervient en la matière[246]. Nous plaidons en faveur d'une augmentation de la coopération internationale et de la rapidité des procédures mais il nous semble que pour que soit acceptable la recherche internationale sur les réseaux sans autorisation de la part du pays où se situe une partie de ce réseau, une convention internationale doit régir la matière.

Section IV. L'injonction de produire

Les articles 88*quater* et 90*quater* du Code d'instruction criminelle prévoient une obligation de produire des informations et de coopérer avec les autorités de recherche. Cette obligation fut, plus tard, également prévue par la Convention de Budapest[247].

---

[241] C. DE VALKENEER, « Manuel de l'enquête pénale », Bruxelles, Larcier, 2005, p. 450.
[242] *Ibidem*
[243] C.i.cr., art. 88*ter*.
[244] C.i.cr., art. 88*ter*.
[245] Il s'agit par exemple des commissions rogatoires.
[246] Une grande partie de la doctrine, ainsi que le Conseil d'État se sont également prononcé dans ce sens. Projet de loi du 28 novembre 2000 relative à la criminalité informatique, exposé des motifs, *Doc. Parl.*, Chambre, n° 0213/001, p. 23.
[247] La Convention de Budapest prévoit cette obligation dans ses articles 18 et 19.

Bien que la loi transposant la directive européenne sur la rétention des données fut déclarée inconstitutionnelle[248], il n'en reste pas moins que certaines données sont stockées durant un certain temps dans les serveurs informatiques[249]. Celles-ci peuvent être très utiles à la recherche d'infractions et d'indices pour identifier des personnes ou pour rechercher des preuves de délits commis sur Internet.

À cette fin le législateur a instauré l'obligation pour toute personne supposée avoir une connaissance particulière du système informatique faisant l'objet de la recherche de collaborer et de fournir des informations sur ce système informatique[250]. Les personnes supposées avoir une connaissance particulière de la façon de protéger ou de crypter les données au sein de ce service informatique peuvent également faire l'objet de cette injonction de collaboration[251]. Le refus de collaboration est sanctionné.

Cet article n'est pas applicable aux suspects en vertu du droit au silence[252]. Les personnes relevant de l'article 156 du Code d'instruction criminelle échappent également à cette injonction[253].

Les articles 88*quater* et 90*quater* du Code d'instruction criminelle sont extrêmement utiles dans un pays dans lequel la liberté de crypter est consacrée. J. Kerkhofs admet que la liberté de crypter comporte de nombreux avantages dans des domaines tels que la sécurité de l'*e-banking* mais qu'elle va également de pair avec des effets désastreux[254]. En effet, contrairement à nos voisins français qui ne connaissent pas une liberté de crypter aussi large, la Belgique permet aux cybercriminels de rendre leurs données illisibles par les autorités de recherche sans les obliger à fournir une clé de décryptage afin de convertir les données encryptées en données compréhensibles. Les obligations des articles 88*quater* et 90*quater* C.i.cr. permettent aux autorités de recherche d'obliger certaines personnes à collaborer à l'enquête afin de pouvoir décrypter les informations.

Il est donc possible de pallier à ces problèmes au moyen des articles 88*quater* et 90*quater* du Code d'instruction criminelle, ce qui fait que cet article est indispensable en droit belge.

---

[248] C.C., 11 juin 2015, n° 84/2015.
[249] Art. 126 de la loi du 13 juin 2005 relative aux communications électroniques, *M.B.*, 20 juin 2005.
[250] C.i.cr., art. 88*quater*.
[251] C.i.cr., art. 90*quater*.
[252] Art. 14.3.g. du Pacte international relatif aux droits civils et politiques, conclu à New York le 16 décembre 1966, approuvé par la loi belge du 15 mai 1981, *M.B.*, 6 juillet 1986. Pour plus d'informations concernant l'étendue de ce droit, voy. M.-A. BEERNAERT, N. COLETTE-BASECQZ, CH. GUILLAIN, *et al.*, *Introduction à la procédure pénale*, 3e éd., Bruxelles, La Charte, 2011.
[253] C. DE VALKENEER, *op. cit.*, p. 450.
[254] J. KERKHOFS et PH. VAN LINDHOUT, « Cybercriminaliteit doorgelicht », *op. cit.*, p. 192.

Toutefois, dans de nombreux cas, ce ne sont pas les personnes visées par les articles 88*quater* et 90*quater* qui ont crypté les données et celles-ci ne sont alors d'aucune utilité à l'enquête. Lorsque les cybercriminels procèdent eux-mêmes au cryptage de leurs données et refusent ensuite de collaborer et de livrer la clé de cryptage, les enquêteurs se trouvent dans une impasse et l'enquête ne peut plus continuer[255]. Les cyberdélinquants ne peuvent pas être obligés de livrer cette clé en vertu du droit de ne pas s'incriminer soi-même[256].

Selon J. Kerkhofs une possible solution, outre le fait de renoncer à la liberté de cryptage, serait d'avoir une centrale qui rassemble toutes les clés de cryptage et qui, sur ordre judiciaire, devrait délivrer la clé adéquate à la justice sans quoi on laisse une trop grande porte ouverte aux cybercriminels[257].

Le FCCU s'aligne sur l'avis de J. Kerkhofs et l'inspecteur principal, Koen Smets, affirme que la liberté de crypter est un des plus gros problèmes à l'efficacité des recherches du FCCU. Sans une centrale rassemblant les clés de cryptage, lorsque les cyberdélinquants auront acquis encore plus de connaissance en matière de cryptage et crypteront eux-mêmes leurs données, les enquêtes ne pourront plus être effectives[258].

Section V. L'obligation de collaboration

Un autre sérieux problème du cybermonde est l'anonymat. En effet, bien que ce dernier soit plus faible qu'on ne pourrait le croire, l'impression d'anonymat sur les réseaux mène à plus de criminalité[259]. Les auteurs ont l'impression d'être intraçables et de pouvoir agir en toute impunité, surtout depuis la création du logiciel TOR[260].

Ce n'est que récemment qu'un mécanisme pour faciliter l'identification des auteurs à travers leurs adresses IP fut mis en place. Avant cela, les auteurs qui disposaient d'un minimum de connaissances en informatique, pouvaient s'assurer de commettre des délits en toute impunité.

[255] Voy. annexe n° 1, question 14 de la retranscription de l'entretien avec Koen SMETS et Marjolein DELPLACE, du FCCU.
[256] C. DE VALKENEER, *op. cit.*, p. 450.
[257] J. KERKHOFS et PH. VAN LINDHOUT, « Cybercriminaliteit doorgelicht », *op. cit.*, p. 193.
[258] Voy. annexe n° 1, question 14 de la retranscription de l'entretien avec Koen SMETS et Marjolein DELPLACE, du FCCU.
[259] J. CLOUGH, *Principles of cybercrime*, Cambridge, Cambridge University Press, 2010, pp. 5 à 6.
[260] TOR est l'acronyme utilisé pour *The Onion Router*, logiciel permettant d'assurer un anonymat sur le *dark web*.

En 2007[261], le législateur a incorporé dans le Code d'instruction criminelle un article 46*bis* prévoyant une obligation de collaboration dans le cybermonde[262]. Cet article oblige l'opérateur d'un réseau de communication électronique ou d'un fournisseur de services de communications électroniques de collaborer afin de permettre d'identifier l'utilisateur d'un système informatique. Le refus de collaboration étant lourdement sanctionné par une amende.

Lorsque l'opérateur d'un réseau de communication électronique ou d'un fournisseur de service de communication électronique est établi sur le sol belge, cet article fonctionne relativement bien et aide énormément les autorités de recherche dans leurs enquêtes.

Sur le plan international, la collaboration est également efficace avec certains acteurs économiques tels que *Microsoft* ou *Facebook*[263]. Toutefois, avec d'autres acteurs la collaboration n'est pas simple car différentes interprétations existent quant au champ d'application personnel de l'article. La saga judiciaire *Yahoo !* en est un bel exemple.

En l'espèce il s'agissait d'auteurs ayant réalisé des délits sur Internet au moyen d'adresses *Yahoo!* avec des identités fictives. Le procureur du Roi belge décida, sur base de l'article 46*bis* C.i.cr., d'obliger la compagnie américaine *Yahoo!* de fournir des informations permettant d'identifier les auteurs en ce que les adresses *Yahoo!* étaient accessibles en Belgique. Selon le procureur du Roi belge, la compagnie *Yahoo!* ne se situait pas physiquement en Belgique, mais bien virtuellement, ce qui la soumettait à l'obligation de l'article 46*bis* du Code d'instruction criminelle. *Yahoo !* refusa en estimant ne pas être soumis à cette obligation.

La saga *Yahoo!* a connu plusieurs phases. Dans un premier temps, l'affaire fut fixée devant le tribunal correctionnel de Termonde en mars 2009[264]. Le tribunal estima que l'entreprise *Yahoo!*, bien que non présente physiquement en Belgique était visé par l'article 46*bis* du Code d'instruction criminelle étant donné que ses services étaient disponibles en Belgique et elle aurait, dès lors, dû se soumettre à l'obligation de collaboration. « Une demande d'entraide

[261] Loi du 23 janvier 2007 portant dispositions diverses, *M.B.,* 14 mars 2014.
[262] Il convient de distinguer l'obligation de collaboration dans le cybermonde instauré à l'article 46*bis* C.i.cr. de l'injonction de produire de l'article 88*quater* et 90*quater* C.i.cr.
L'obligation de coopération consiste en une obligation pour l'opérateur d'un réseau de communication électronique ou d'un fournisseur de service de communication électronique de fournir à la demande des autorités compétentes des indications permettant d'identifier un utilisateur du réseau. Il s'agit principalement de dévoiler le nom d'un détenteur d'une adresse IP, d'une adresse *e-mail,* d'un numéro IMEI.
L'injonction de produire, quant à elle, consiste en une obligation pour toute personne ayant une connaissance particulière du système faisant l'objet de la recherche de collaborer avec les autorités compétentes afin de dévoiler des informations quand au fonctionnement d'un système informatique et à la manière d'accéder à son contenu. Il s'agit principalement de dévoiler des clés de cryptage.
[263] Voy. annexe n° 1, question 5 de la retranscription de l'entretien avec l'inspecteur Koen SMETS et l'analyste stratégique du FCCU, Marjoleine DELPLACE.
[264] Corr. Termonde, 2 mars 2009, *T. Strafr.*, 2009, vol. 2, p. 116.

judiciaire n'aurait pas été nécessaire dès lors que les données demandées […] avaient traits à un trafic électronique en Belgique »[265].

L'entreprise américaine fit appel contre cette décision et l'affaire fut renvoyée devant la Cour d'appel de Gand[266]. Celle-ci eut une autre approche du problème et réforma la décision rendue en première instance. La Cour d'appel de Gand estima que *Yahoo!* était une entreprise américaine et que les services de celle-ci étaient disponibles en Belgique uniquement grâce à des opérateurs de réseaux et de fournisseurs de communications électroniques belges qui permettent que les services de *Yahoo!* soient rendus virtuellement accessibles en Belgique[267]. *Yahoo!* ne faisait qu'utiliser l'infrastructure du réseau belge, mais ne peut pas être considéré comme une entreprise belge fournissant des services de communications électroniques[268].

Le parquet général de Gand introduit un premier pourvoi en cassation en 2011[269] « rejetant précisément cette assimilation [au nom de] l'autonomie conceptuelle du droit pénal »[270]. Celui-ci mena à la cassation de la décision de la Cour d'appel de Gand. L'arrêt de cassation affirmait que l'obligation de collaboration prévue dans l'article 46*bis* du Code d'instruction criminelle s'appliquait à toute personne qui offrait un service permettant d'échanger des informations au moyen d'un réseau de communication électronique[271]. Ainsi l'affaire fut cassée et renvoyée devant la Cour d'appel de Bruxelles.

Devant la Cour d'appel de Bruxelles[272], la saga continua car la Cour ne s'aligna pas entièrement sur la décision de la Cour de cassation. La Cour d'appel s'estima compétente, ce qui implique qu'elle a « vraisemblablement considéré *Yahoo !* comme étant un prestataire de service en Belgique »[273]. Toutefois, elle estima que la demande de collaboration était invalide car elle avait été envoyée à une entreprise se situant hors des frontières belges et non à la société et non à la société *Yahoo !* en Belgique.

---

[265] O. LEROUX, « Arnaques, fraudes et escroqueries sur internet : moyens concrets d'investigation. Point sur l'affaire dite *Yahoo* ! à la suite du second arrêt de la Cour de cassation », *op. cit.*, p. 841.
[266] Gand, 30 juin 2010, *T. Strafr.*, 2011, vol. 2, p. 132.
[267] K. DE SCHEPPER et F. VERBRUGGEN, « Ontsnappen *space invaders* aan onze *pacmannen?* De materiële en formele strafrechtsmacht van België bij een strafbare weigering van medewerking door elektronische dienstverleners », *T. Strafr.*, 2013, vol. 3, p. 145.
[268] *Ibidem ;* la Cour estime que ces notions doivent s'interpréter selon leur sens reçu dans la loi du 13 juin 2005 relative aux communications électroniques.
[269] Cass., 18 janvier 2011, *T. Strafr.*, 2011, vol. 2., p. 120.
[270] O. LEROUX, « Arnaques, fraudes et escroqueries sur internet : moyens concrets d'investigation. Point sur l'affaire dite *Yahoo !* à la suite du second arrêt de la Cour de cassation », *op. cit.*, p.842.
[271] K. DE SCHEPPER et F. VERBRUGGEN, *op. cit.*, p. 146.
[272] Bruxelles, 12 octobre 2011, *A&M*, 2012, vol. 2-3, p. 238 cité dans K. DE SCHEPPER et F. VERBRUGGEN, *op. cit.*, p. 146.
[273] *Ibidem*

A nouveau, le ministère public fit un second pourvoi en cassation. Et l'arrêt de la Cour d'appel de Bruxelles fut cassé. En effet, la Cour déclara que « La circonstance que le procureur du Roi envoie depuis la Belgique à une adresse établie à l'étranger sa demande écrite visée à l'article 46*bis* du Code d'instruction criminelle, requérant le concours d'un opérateur de réseau de communication électronique établi en dehors du territoire belge ou du fournisseur d'un service de communication électronique, n'invalide pas cette demande »[274]. Bien que la Cour de cassation estima que la demande sur base de l'article 46*bis* du Code d'instruction criminelle était valable, celle-ci ne se prononça pas sur le caractère obligatoire ou non pour un fournisseur ou opérateur étranger de fournir ces informations.

Suite à l'arrêt de cassation, l'affaire fut renvoyée une dernière fois devant la Cour d'appel d'Anvers[275] qui vint, une fois pour toutes, clôturer le débat concernant le champ d'application *ratione personae* du devoir de coopération prévu dans l'article 46*bis* du Code d'instruction criminelle.

L'arrêt de la Cour d'appel d'Anvers a estimé que l'article 46*bis* du Code d'instruction criminelle s'appliquait à *Yahoo!* étant donné que *Yahoo!* était virtuellement localisé en Belgique vu que l'entreprise offrait des services de communications électroniques. Elle s'aligne ainsi sur la décision qui fut rendue par le tribunal de première instance de Termonde.

En résumé, on peut tirer comme enseignement de cette saga judiciaire que la simple présence virtuelle en Belgique permet de soumettre un opérateur ou un fournisseur de services de communications électroniques à l'obligation de collaboration.

Une affaire *Skype* présentant de nombreuses similarités avec l'affaire *Yahoo !*[276] est actuellement pendante devant le tribunal correctionnel de Malines. Cette affaire pourrait venir confirmer ou infirmer la jurisprudence *Yahoo !* et donner plus d'informations quant à cette obligation de coopération. Cette affaire est très attendue par la doctrine belge. Toutefois, rien ne garantit que l'affaire soit jugée rapidement en raison de l'introduction d'un pourvoi en

[274] Cass., 4 septembre 2012, inédit, cité dans O. LEROUX, « Arnaques, fraudes et escroqueries sur internet : moyens concrets d'investigation. Point sur l'affaire dite *Yahoo* ! à la suite du second arrêt de la Cour de cassation », *op. cit.*, p.842. Traduction du passage: « De omstandigheid dat de procureur des Konings zijn door artikel 46*bis* Wetboek van Strafvordering bedoelde schriftelijke vordering, waarbij de medewerking wordt gevorderd van een buiten het Belgisch grondgebied gevestigde operator van een elektronisch communicatienetwerk of van de verstrekker van een elektronische communicatie dienst, verstuurt vanuit België aan een in het buitenland gelegen adres, maakt die vordering niet ongeldig ».

[275] Anvers (12e ch.), 20 novembre 2013, Anvers, 20 novembre 2013, *T.Strafr.*, 2014, p. 75.

[276] Rédaction en ligne, « Skype devant la justice à Malines, l'entreprise se pourvoit en cassation », 10 juin 2015, disponible sur : http://www.lesoir.be/.

cassation pour violation de la présomption d'innocence suite à des déclarations d'un des magistrats à la presse[277].

Chapitre II. L'efficacité de la recherche par les *Computer Crime Units*

Bien qu'une immense majorité des belges, et des européens en général, disposent d'un accès à Internet, la connaissance de la plupart d'entre eux en matière de sécurité et de protection des systèmes informatiques reste très limitée. Il en va de même pour le personnel policier et pour les magistrats.

La recherche et la poursuite des infractions en matière de cybercriminalité ne pouvaient pas être efficaces sans la mise à disposition de moyens techniques et adaptés, de formations pour la police et les magistrats et de la mise en place de départements experts en la matière. Pour cette raison, différents *Computer Crime Units* furent mis en place.

Nous analyserons brièvement les différents *Computer Crime Units* (Section I) et jetterons un regard critique sur ces institutions (Section II).

Section I. Les autorités spécialisées pour la recherche de la criminalité informatique

Avant l'entrée en vigueur de la loi du 28 novembre 2000, la nécessité se faisait déjà ressentir en Belgique de créer des entités spécialisées pour la recherche des infractions commises par le biais des nouvelles technologies.

Au sein de la police judiciaire divers *Computer Crime Units* furent successivement créés à partir du début des années nonante[278]. Ceci mena, avec la réforme de services de police de 1998, à la création du *Federal Computer Crime Unit (FCCU)*. Il s'agit de la première unité fédérale spécialisée dans la recherche de la criminalité informatique. A côté de celle-ci, subsistent les *Regional Computer Crime Units* (RCCU) qui furent créés quelques années auparavant.

La recherche de la criminalité informatique existe à plusieurs niveaux. Au niveau fédéral, le FCCU s'occupe des affaires de cybercriminalité les plus importantes et les plus complexes[279]. Les RCCU, au niveau régional, sont responsable de la « qualité des analyses ICT légales de PC

[277] Rédaction en ligne, « Skype devant la justice à Malines, l'entreprise se pourvoit en cassation », 10 juin 2015, disponible sur : http://www.lesoir.be/.
[278] K. VERHAEGHE, *op. cit.*, p. 99.
[279] Pour plus d'informations, voy. : http://www.police.be/fed/fr/.

et autres supports de données et petits réseaux. Les RCCU recherchent les traces de criminalité sur Internet et identifient les auteurs »[280]. Ils peuvent se faire aider dans leur tâche par le FCCU. Environ 90% des recherches des RCCU consistent à aider la police locale dans la recherche de preuves et l'identification de suspects pour des infractions de cybercriminalité non-spécifique. Seuls 10% de leur capacité de recherche sont dédiés à la cybercriminalité spécifique[281]. Ceci est dû au manque de moyens et de formation de la police locale.

Étant donné la complexité de la cybercriminalité, l'enquête se déroule par de nombreux allers-retours entre le ministère public et les entités spécialisées[282]. Le FCCU dispose d'une capacité d'enquête autonome et fait des rapports au ministère public.

Récemment des discussions évoquaient une possibilité de régionaliser entièrement les *Cyber Crime Units* de sorte que le FCCU disparaîtrait. Ceci suscita de vives réactions dans le milieu judiciaire et il se pourrait que, grâce à cela, le projet ne soit pas mis en œuvre[283].

Section II. Regard critique sur l'institution du FCCU

Bien que la cybercriminalité soit considérée comme un phénomène de criminalité prioritaire par le Plan National de Sécurité[284], l'octroi de moyens suffisants aux entités de recherche ne semble pas en être un. Tant le FCCU que les RCCU et la police locale ne disposent pas de moyens suffisants afin de travailler de manière optimale.

Lors d'une interview accordée en 2011, Luc Beirens, ancien directeur de la FCCU, déclare qu'au niveau des connaissances, le FCCU peut se mesurer à n'importe quel autre *Computer Crime Unit* étranger[285]. Toutefois, ce dernier affirme qu'en termes de budget, de matériel et de personnel, la Belgique est loin en dessous de ses voisins européens et que cela affecte sensiblement l'efficacité de son service[286].

L'inspecteur principal Koen Smets et Marjolein Delplace, l'analyste stratégique du FCCU, expriment leur désespoir face à cette situation difficile. Le FCCU compte seulement 31

[280] Information disponible sur le site de la police fédérale, voy. : http://www.police.be/fed/fr/.
[281] Voy. annexe n° 1, question 7 de la retranscription de l'entretien avec l'inspecteur Koen SMETS, et l'analyste stratégique du FCCU, Marjolein DELPLACE.
[282] Voy. annexe n° 1, question 4 de la retranscription de l'entretien avec l'inspecteur Koen SMETS, et l'analyste stratégique du FCCU, Marjolein DELPLACE.
[283] Voy. annexe n° 1, question 13 de la retranscription de l'entretien avec l'inspecteur Koen SMETS, et l'analyste stratégique du FCCU, Marjolein DELPLACE.
[284] Plan National de Sécurité 2012-2015 disponible sur : http://www.police.be/files/fed/files/ORG/INT/PNS2012-2015.pdf, pp. 15 à 16.
[285] Voy. annexe n° 2, question 7 de la retranscription de l'entretien avec l'ancien directeur du FCCU, Luc BEIRENS.
[286] Voy. annexe n° 2, question 7 de la retranscription de l'entretien avec l'ancien directeur du FCCU, Luc BEIRENS.

membres pour faire les recherches en matière de cybercriminalité, le tout avec des moyens financiers très limités et un matériel relativement désuet[287].

Alors que le gouvernement avait approuvé une augmentation du budget de ces entités de recherche, ils n'en ont pas bénéficié suite à un « oubli »[288]. Le découragement est bel et bien présent au sein du FCCU.

Lorsqu'un fait de cybercriminalité important se retrouve étalé dans la presse, comme ce fut le cas avec l'affaire *Belgacom*¸ le gouvernement fait de belles promesses concernant l'augmentation du budget consacré à la lutte en la matière. Toutefois, ces bonnes résolutions disparaissent aussi vite que l'attention médiatique accordée au problème[289].

Un changement de mentalité devrait avoir lieu au sein du gouvernement et du monde politique dans son ensemble afin de réellement considérer la cybercriminalité comme une des grandes menaces de notre époque et de permettre de libérer un budget pour lutter plus efficacement contre cette forme de criminalité.

Outre une augmentation en termes de moyens financiers, matériels et de personnel, d'autres améliorations pourraient voir le jour pour favoriser l'efficacité des recherches par les *Computer Crime Units.*

La principale, à notre sens, serait d'assouplir les conditions des méthodes particulières de recherches afin de permettre aux policiers du FCCU d'avoir recours à l'infiltration. Des négociations à ce sujet sont en cours actuellement[290] et nous espérons un changement.

Chapitre IV. Efficacité de la poursuite

Afin d'étudier l'efficacité de la poursuite en terme de cybercriminalité, il convient de prendre en compte la politique criminelle menée par le Parquet (Section I). Nous aborderons ensuite brièvement l'impunité de fait dont jouissent les délits de presse informatiques (Section II). Enfin

[287] Voy. annexe n° 1, question 7 de la retranscription de l'entretien avec l'inspecteur Koen SMETS, et l'analyste stratégique du FCCU, Marjolein DELPLACE.
[288] Voy. annexe n° 1, question 7 de la retranscription de l'entretien avec l'inspecteur Koen SMETS, et l'analyste stratégique du FCCU, Marjolein DELPLACE.
[289] Voy. annexe n° 1, question 7 de la retranscription de l'entretien avec l'inspecteur Koen SMETS, et l'analyste stratégique du FCCU, Marjolein DELPLACE.
[290] Voy. annexe n° 1, question 2 de la retranscription de l'entretien avec l'inspecteur Koen SMETS, et l'analyste stratégique du FCCU, Marjolein DELPLACE.

nous analyserons les statistiques du ministère public (Section III) et tirerons des conséquences sur l'efficacité des poursuites.

Section I. La politique criminelle

Il convient de se demander après la recherche des infractions, dans quelle mesure celles-ci sont effectivement poursuivies. Il s'agit d'une question d'efficacité des poursuites mais également de politique criminelle.

Depuis la fin des années '90 mais surtout depuis le début des années 2000, la cybercriminalité a fait son apparition dans les circulaires ministérielles et circulaires du collège des procureurs généraux en matière de politique criminelle[291]. On peut noter que la répression semble plus axée sur certains cyberdélits que sur d'autres.

Ces dernières années, les circulaires du collège des procureurs généraux insistent sur la collaboration internet pour la recherche et la poursuite de la cybercriminalité et aussi sur la collaboration internationale[292]. Leur but est de réduire au maximum les difficultés éprouvées en termes de coopération et d'ainsi permettre une lutte plus adéquate contre la cybercriminalité.

Le nombre de circulaires se préoccupant du problème de cybercriminalité sont élevées et témoignent d'une prise de conscience du ministère public de la nécessité de réprimer les délits de l'environnement numérique[293].

Section II. Le cas de l'impunité pénale du délit de presse

Dans le cadre de ce chapitre sur l'efficacité de la poursuite pénale, nous souhaitons également aborder très brièvement la problématique du délit de presse.

Tout d'abord, il convient de préciser que le délit de presse est tout délit ordinaire – tels que par exemple la calomnie, la diffamation etc. – commis par voie de presse[294]. Il ne s'agit donc pas d'un délit spécifique, mais d'un mode d'exécution d'un délit ordinaire.

---

[291] Différentes circulaires abordent la question depuis 1999. La première circulaire avec une réelle importance en la matière fut celle du Collège des Procureurs généraux du 14 février 2002, disponible sur : http://www.om-mp.be/circulaires.html.

[292] À titre d'exemple nous pouvons retenir la ciruclaire 21/2010 du 25 novembre 2010 relative à la coopération internationale en matière pénale. Cette circulaire est disponble sur : http://www.om-mp.be/omzendbrief/4582116/col_21-2010_dd__25_11_2010.html.

[293] Plus d'informations à propos des circulaires peut être trouvé sur le site du ministère public : http://www.om-mp.be/circulaires.html.

[294] M. GIACOMETTI et P. MONVILLE, « Réseaux sociaux, anonymat et faux profils : vrais problèmes en droit pénal et de la procédure pénale », *Les réseaux sociaux et le droit »*, sous la direction de M. SALMON, Bruxelles, Larcier, 2014, p. 184.

En raison de la liberté de la presse, qui est un des principes fondamentaux de notre état de droit, le régime encadrant les délits de presse est particulièrement protecteur[295]. La principale caractéristique de ce régime consiste en le fait qu'un « délit de presse emporte […] la compétence du jury d'assises pour en connaître »[296]. Étant donné le caractère très lourd d'une procédure d'assises, il est extrêmement rare que le ministère public décide de poursuivre un délit de presse, hormis dans les cas d'un délit de presse à caractère raciste et xénophobe qui, quant à eux, relèvent de la compétence du tribunal correctionnel[297].

Cette impunité *de facto* ne posait pas de réel problème jusqu'il y a peu. En effet, alors que depuis 1831 – date de l'entrée en vigueur de la constitution –le délit de presse sanctionnait uniquement les délits commis par voie de presse écrite traditionnelle, une révolution vit le jour en 2012. Un arrêt de la Cour de cassation du 6 mars 2012 opéra une modernisation de la notion de presse écrite en permettant que des écrits informatiques rentrent dans le champ d'application du délit de presse.

Cette modernisation permis non seulement à des versions électroniques de quotidiens et autres journaux d'entrer dans son champ d'application, mais le permis également à des statuts Facebook ou opinions sur Twitter.

Alors qu'autrefois les personnes bénéficiant de l'impunité *de facto* accordée au délit de presse étaient minoritaires[298], cette impunité est aujourd'hui accordée à un échantillon de la population beaucoup plus large. « D'un milieu essentiellement composé de professionnels et au sein duquel les acteurs étaient peu nombreux et généralement soucieux des valeurs de la déontologie journalistique, nous sommes passés sans transition à un environnement dans lequel les auteurs potentiels de délits de presse se comptent désormais par millions »[299].

Nous sommes conscients du fait qu'il y a une politique criminelle à respecter et qu'il est totalement impossible de poursuivre tous les délits de presse commis sur Internet, et plus particulièrement sur les réseaux sociaux. Toutefois, l'impunité *de facto* dont jouissent tous ces délits nous semble inacceptable et un gros problème de procédure pénale belge.

---

[295] C. BEHRENDT « Le délit de presse à l'ère numérique », *R.B.D.C.*, 2014, p. 305.
[296] *Ibidem*
[297] Constitution, art. 150.
[298] Il s'agissait principalement de journalistes et les délits étaient peu fréquents étant donné les codes de déontologies que ceux-ci se voient contraints de respecter.
[299] C. BEHRENDT, *op. cit.*, p. 310.

Nous espérons qu'une réforme aura lieu prochainement afin que les délits de presse commis sur Internet, n'échappent pas d'office à une poursuite pénale. Il ne s'agit plus des quelques rares délits de presse annuels d'avant 2012, mais nous parlons désormais de nombres beaucoup plus élevés. Une impunité *de facto* pour tous ces délits est à notre sens totalement inacceptable.

Toutefois, ceci nécessite une réforme en profondeur, car il nous semble également qu'une personne rédigeant un statut injurieux sur un réseau social ne devrait pas risquer le jugement par un jury d'assises. Toutefois, nous nous engageons là dans une problématique distincte…

Section III. Analyse des statistiques

Afin de pouvoir donner une opinion éclairée sur la question de l'efficacité de la procédure pénale belge en termes de cybercriminalité, il convient d'analyser les statistiques recueillies annuellement par le ministère public. À travers ces statistiques nous pouvons analyser le flux d'entrée et le flux de sortie des affaires en relation avec la cybercriminalité afin d'en tirer des conséquences quant à l'efficacité des poursuites.

Il convient de relever que sous la classification « informatique », toute la cybercriminalité n'est pas regroupée. En effet, seule la cybercriminalité spécifique sera reprise sous ce vocable alors que la criminalité non-spécifique sera reprise sous le vocable de son pendant traditionnel. Bien que cette catégorie n'englobe donc pas toute la cybercriminalité, elle est intéressante afin d'évaluer l'efficacité des poursuites.

En 2014, 18.892 affaires de cybercriminalité spécifique furent constatées[300]. Ce nombre a très peu varié depuis 2010, mais a quasiment doublé depuis 2008[301]. En dix ans, le nombre d'infractions rencontrées en matière de cybercriminalité s'est multiplié par 18[302]. Cette augmentation traduit d'une part l'augmentation réelle de la cybercriminalité, mais également une politique criminelle prenant de plus en plus en compte cette facette de la criminalité.

Il convient de préciser que ce nombre d'infractions n'est pas représentatif de toute la cybercriminalité. Outre le fait qu'il ne s'agisse que de la cybercriminalité spécifique, il existe, comme dans toute criminalité, un chiffre noir. C'est-à-dire qu'un volet de la cybercriminalité ne rentre pas dans les statistiques car il n'est pas dénoncé par les victimes, ni rencontré par les autorités de recherche.

[300] Voy. annexe n° 4, statistiques en matière de criminalité informatique spécifique – Flux d'entrée 2014.
[301] Voy. annexe n° 9, statistiques en matière de criminalité informatique spécifique – Flux d'entrée 2003 à 2014.
[302] Voy. annexe n° 9, statistiques en matière de criminalité informatique spécifique – Flux d'entrée 2003 à 2014.

Le nombre d'affaires pendantes en 2014 est de 5.155 affaires[303]. Le nombre d'affaires pendantes augmente sensiblement chaque année mais ceci n'est pas uniquement un signe d'inefficacité. Ce chiffre traduit plus spécifiquement une corrélation avec l'augmentation annuelle de cybercriminalité ainsi qu'une enquête approfondie.

En 2014, le flux de sortie en matière de cybercriminalité spécifique compte 18.029 affaires[304] et nous révèle plusieurs informations importantes. 12.000 de ces affaires furent classées sans suite. 1.728 affaires furent transmises pour disposition à un autre parquet. 3.992 affaires furent jointes à une affaire-mère. Seules 6 affaires firent l'objet d'une transaction payée et 47 furent l'objet d'une médiation aboutie. Une citation directe eu lieu dans seulement 132 affaires. La chambre du conseil fut saisie de 124 affaires[305].

Une information importante qui ressort de ces statistiques est le fait 66,55% du flux de sortie sont des classements sans suite[306]. Ceci est un taux relativement élevé qui s'explique par le fait qu'à l'heure d'aujourd'hui il est encore très difficile d'effectuer des enquêtes approfondies dans le cybermonde qui aboutissent à des indices suffisants pour pouvoir poursuivre effectivement les auteurs de cyberdélits. Selon Marjolein Delplace, analyste stratégique du FCCU, ces classements sans suite sont principalement dus à une non-identification de l'auteur.

Toutefois, en comparaison avec le pourcentage de classements sans suite de la criminalité en général[307], il n'y a rien d'inquiétant. Il est normal qu'une partie de la criminalité soit classée sans suite pour des motifs d'opportunité ou pour des motifs techniques tels que l'absence de charges suffisantes envers un auteur.

L'augmentation des effectifs d'enquête au sein du FCCU, ainsi que la formation de personnel supplémentaire permettrait de bénéficier d'enquêtes plus poussées et d'éviter certains classements sans suite pour des motifs tels que l'absence de charges suffisantes etc. Mais ce pourcentage ne sera jamais réduit à néant.

Une autre information importante qui ressort des statistiques est le fait que seuls 0,73% des affaires de cybercriminalité spécifique mènent à une citation directe[308]. En comparaison avec

[303] Voy. annexe n° 3, statistiques en matière de criminalité informatique spécifique – Affaires pendantes 2014.
[304] Voy. annexe n° 5, statistiques en matière de criminalité informatique spécifique – Flux de sortie 2014.
[305] Voy. annexe n° 5, statistiques en matière de criminalité informatique spécifique – Flux de sortie 2014.
[306] Nous obtenons ce pourcentage en divisant 12.000 par 18.029 et multipliant par 100. Pour plus d'informations, voy. annexe n° 5, statistiques en matière de criminalité informatique spécifique – Flux de sortie 2014.
[307] Voy. annexe n° 5, statistiques en matière de criminalité informatique spécifique – Flux de sortie 2014.
[308] Nous obtenons ce pourcentage en divisant 132 par 18.029 et multipliant par 100. Pour plus d'informations, voy. annexe n° 5, statistiques en matière de criminalité informatique spécifique – Flux de sortie 2014.

la criminalité en général dans laquelle le flux de sortie menant à une citation directe est du quadruple[309], on peut affirmer qu'il y a encore des efforts à faire pour poursuivre activement la cybercriminalité.

Une autre remarque quant à l'efficacité des poursuites est pointée du doigt par Luc Beirens, ancien directeur du FCCU. Il souligne que dans l'immense majorité des cas où une infraction de cybercriminalité comporte un élément international, la poursuite n'est que très rarement effective. Toutefois, nous ne disposons pas de statistiques assez précises afin de pouvoir confirmer ces affirmations.

En guise de conclusion, le droit de la procédure pénale, est-il efficace ?

En termes de législation, nous pouvons dans l'ensemble féliciter notre législateur d'avoir mis en place une adaptation efficace de la procédure pénale traditionnelle à une réalité totalement différente. Des efforts sont encore à faire par la communauté internationale pour tenter d'augmenter l'harmonisation procédurale, la coopération internationale et la rapidité des procédures. Mais nous sommes sur la bonne voie.

Les autorités de recherches sont actuellement confrontées à un manque criant de moyens. Ceci a comme conséquence que, même si les procédures prévues par la législation belge sont dans l'ensemble un succès et permettraient de rechercher et poursuivre efficacement les infractions, les autorités de recherches ne peuvent pas travailler à 100% de leur potentiel ce qui est regrettable.

Au niveau de la poursuite, les statistiques ne sont pas alarmantes. Nous espérons toutefois voir augmenter le pourcentage de citations directes dans les années à venir.

[309] Pour l'ensemble de la criminalité, le flux de sortie comportait un taux de citation directe de 2,94%. Nous obtenons ce pourcentage en divisant 19.630 par 667.038 puis multipliant par 100. Pour plus d'informations, voy. annexe n° 5, statistiques en matière de criminalité informatique spécifique – Flux de sortie.

CONCLUSION GÉNÉRALE

« La cybercriminalité est la troisième grande menace pour les grandes puissances, après les armes chimiques, bactériologiques et nucléaires »[310] clamait Colin ROSE en 2000 en espérant conscientiser la société à l'avènement de ce phénomène croissant – et il ne s'était pas trompé.

La cybercriminalité fait quotidiennement de nombreuses victimes et, de jour en jour, les cybercriminels prennent de plus en plus de pouvoir au sein de notre société de l'information.

De l'analyse des dispositions pertinentes en la matière, nous pouvons tirer plusieurs conclusions quant à l'effectivité de la législation pénale qui encadre la cybercriminalité.

Principalement introduite en 2000, avec un certain empressement, et très peu modifiée depuis, la législation pertinente à propos de la cybercriminalité est marquée par une imprécision déplorable. En effet, tant dans les définitions des infractions que dans les nouveaux articles régissant la procédure pénale du cybermonde, l'imprécision est manifeste.

Bien entendu, une partie de l'imprécision fut volontaire en raison de la nécessité d'une terminologie techniquement neutre permettant d'adapter la législation à une réalité virtuelle qui évolue très rapidement. Cependant, d'après nous, des concepts-clés sont définis de manière trop vague que pour répondre aux exigences du principe de légalité et il convient d'y remédier.

Outre l'imprécision de la loi, d'autres critiques peuvent être faites tant en ce qui concerne le droit pénal matériel que procédural du cybermonde.

Du point de vue matériel, les nouvelles incriminations sont marquées par un manque de cohérence, l'existence de discriminations et des risques de pénalisations excessives. Et d'un point de vue procédural, nous déplorons la récente annulation de la loi permettant la rétention de données. Nous déplorons également l'absence d'une gestion centrale des clés de cryptage. Et enfin, nous regrettons la lenteur des discussions qui pourraient un jour permettre une infiltration policière sur Internet.

La majorité de ces critiques furent pointées du doigt depuis plusieurs années déjà par la doctrine, mais le législateur n'a toujours pas revu sa copie. Nous sommes face à un domaine qui évolue à une vitesse ahurissante et pourtant nous y répondons par une législation d'une quinzaine

[310] Colin ROSE est un expert en cybercriminalité travaillant pour l'entreprise écossaise Buchanan. Cette citation très connue fut prononcée lors du sommet du G8 à Paris le 15 mai 2000.

d'années d'âge. Il est plus que temps de penser à une actualisation de la législation afin de la mettre à l'ordre du jour et de solutionner les problèmes persistants dans la législation actuelle.

Toutefois, malgré ces nombreuses critiques et notre souhait d'une adaptation législative, il convient de reconnaître que pour une première loi de criminalité informatique, le législateur s'est bien débrouillé. Il a permis d'embraser l'immense majorité des comportements répréhensibles du monde des nouvelles technologies et prévu, dans l'ensemble, une adaptation efficace de la procédure traditionnelle à l'environnement du cybermonde.

C'est vers la communauté internationale que nous nous tournons avec notre critique la plus vive. Celle-ci devrait se battre – plus et plus fort – afin d'améliorer rapidement la coopération internationale pour permettre, de façon plus rapide et plus complète qu'aujourd'hui, d'encadrer ce phénomène grandissant.

Le caractère international est presque intrinsèque à la cybercriminalité et requiert une coopération plus efficace et plus rapide. Bien entendu nous plaidons pour un cadre qui respecterait la souveraineté des états, mais des instruments internationaux de coopération facilitée s'imposent, sans quoi la lutte contre la cybercriminalité deviendra rapidement une tâche impossible.

Nous concluons ce mémoire en disant qu'il est vrai que le législateur belge et la communauté internationale ont encore quelques progrès à faire, mais ils ne sont pas les seuls. Nous, citoyens, pouvons aussi apporter notre pierre à l'édifice et aider dans la lutte contre la cybercriminalité en adoptant un comportement responsable et réfléchi avec les nouvelles technologies. La sécurité dépend également de la prudence et de la responsabilité de chacun.

BIBLIOGRAPHIE

LÉGISLATION

Législation européenne et internationale

- CEDH, art. 7.
- Directive (CE) n° 2006/24 du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, *J.O.U.E.*, L.105/54, 13 avril 2006.
- Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, 28 janvier 2003, Strasbourg, disponible sur : http://conventions.coe.int/Treaty/FR/Treaties/Html/189.htm.
- Convention sur la cybercriminalité, Conseil de l'Europe, signée à Budapest le 23 novembre 2001.
- Pacte international relatif aux droits civils et politiques, conclu à New York le 16 décembre 1966, approuvé par la loi belge du 15 mai 1981, *M.B.*, 6 juillet 1986.
- Recommandation n° R (95) 13 relative aux problèmes de procédure pénale liés à la technologie de l'informatique, adoptée le 11 septembre 1995, éditions du Conseil de l'Europe, 1996, disponible sur http://www.coe.fr/cm/ta/rec/1995/f95r13.htm.
- Recommandation n° R (89) 9 sur la criminalité en relation avec l'ordinateur du 9 septembre 1989, adoptée le 13 septembre 1989, Editions du Conseil de l'Europe, Strasbourg, 1990, disponible sur http://www.coe.fr/cm/ta/rec/1989/f89r9.htm.

Législation belge

- Constitution, art. 12, 14, 25, 150.
- Code pén., art. 193, 210*bis*, 259*bis*, 314*bis*, 461, 491, 496, 504*bis*, 550*bis*, 550*ter*, 504*quater*.
- C.i.cr., art. 39*bis*, 46*bis*, 88*bis*, 88*ter*, 88*quater*, 90*quater*, 90*decies*, 156.

- Loi du 30 juillet 2013 portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90decies du Code d'instruction criminelle, *M.B.,* 23 août 2013.
- Loi du 23 janvier 2007 portant dispositions diverses, *M.B.,* 14 mars 2014.
- Loi du 15 mai 2006 modifiant les articles 259*bis* 314*bis*, 504*bis*, 550*bis* et 550*ter* du Code pénal, *M.B.,* 12 septembre 2006.
- Loi du 13 juin 2005 relative aux communications électroniques, *M.B.,* 20 juin 2005.
- Loi du 28 novembre 2000 relative à la criminalité informatique, *M.B.,* 3 février 2001.
    - Projet de loi du 28 novembre 2000 relative à la criminalité informatique, exposé des motifs, *Doc. Parl.,* Chambre, n° 0213/001.
- Loi du 21 mars 1999 portant réforme à certaines entreprises publiques économiques, *M.B.,* 27 mars 1991.

Législation française

- Code pén. français, art. 323-3.

Législation néerlandaise

- Code pén., art.138a.

Législation luxembourgeoise

- Travaux parlementaires n°349, avis du Conseil d'état Luxembourgeois, pp. 12 à 13, cité dans M. BRAUN, « Les infractions en matière de cybercriminalité », *J.T.L.,* 2011, n° 18, pp. 141 à 154.

DOCTRINE

- ALLEAUME, C., « Les biens numériques, une notion au service du droit ? », *Les technologies de l'information au service des droits : opportunités, défis, limites*, sous la direction de D. LE MÉTAYER, Cahiers du CRID n°32, Bruxelles, Bruylant, 2010, pp. 62 à 84.

- BAEYENS, E., « Een vals profiel op Facebook : de strafrechter vindt niet leuk », *T. Strafr.*, 2012, vol. 2, pp. 104 à 107.

- BAEYENS, E., « Informatica en strafrecht : oude griffels – nieuwe leien », *T. Strafr.*, 2007, vol. 6, pp. 404 à 407.

- BEERNAERT, M.-A., COLETTE-BASECQZ, N., GUILLAIN, CH., *et al., Introduction à la procédure pénale*, 3e éd., Bruxelles, La Charte, 2011.

- BEHRENDT, C., « Le délit de presse à l'ère numérique », *R.B.D.C.*, 2014, pp. 305 à 312.

- BELLON, J., *Droit pénal soviétique et droit pénal occidental*, Paris, Editions de Navarre, cité dans F. TULKENS, e.a., *op. cit.*, p. 230.

- BRAUN, M., « Les infractions en matière de cybercriminalité », *J.T.L.*, 2011, n° 18, pp. 141 à 154.

- CLOUGH, J., *Principles of cybercrime,* Cambridge, Cambridge University Press, 2010, pp. 5 à 6.

- COLLARD, I., « Le juriste peut-il aussi être un cybercriminel ? », *L'informatique, l'Internet et le juriste*, sous la direction de J.-F. HENROTTE, Limal, Anthémis, 2010, pp. 181 à 213.

- CONINGS, C. et VERBRUGGEN, F., « Grondwettelijk Hof plaatst reparateurs dataretentiewet voor moeilijke opdracht », *Juristenkrant*, 2015, n° 312, pp. 1 à 3.

- DE HERT, P., « De wet van 28 november inzake informaticacriminaliteit en het materieel strafrecht. Een wet die te laat komt of een wet die er nooit had moeten komen? », *T. Strafr.*, 2001, pp. 286 à 334.

- DE SCHEPPER, K., et VERBRUGGEN, F., « Ontsnappen *space invaders* aan onze *pacmannen?* De materiële en formele strafrechtsmacht van België bij strafbare weigering van medewerking door elektronische dienstverleners », *T. Strafr.*, 2013, vol. 3, pp. 143 à 166.

- DE VALKENEER, C., « Manuel de l'enquête pénale », Bruxelles, Larcier, 2005.

- DE VEL, G., « La convention sur la cybercriminalité », *Le droit international de l'Internet,* Bruxelles, Bruylant, 2002, p. 238.
- DE VILLENFAGNE, F. et DUSOLLIER, S., « La Belgique sort enfin ses armes contre la cybercriminalité : à propos de la loi du 28 novembre 2000 sur la criminalité informatique », *A&M,* 2001, n°1, pp. 60 à 81.
- DE VILLENFAGNE, F., « Chronique de jurisprudence 2002-2008. Criminalité informatique », *R.D.T.I.,* 2010, n° 39, p. 9 à 28.
- DEBAETS, A., e.a., « Cybercriminaliteit », *Aspecten van europees materieel strafrecht,* sous la direction de G. VERMEULEN, Anvers, Apeldoorn-Maklu, 2002, pp. 381 à 440.
- DEENE, J., « Illegaal kopiëren is geen diefstal », *Juristenkrant,* 2005, n° 102, p. 11.
- EVRARD, S., « La loi du 28 novembre 2000 relative à la criminalité informatique », *J.T.,* 2001, pp. 241 à 245.
- FORGET, C., « La collecte de preuves informatiques en matière pénale », *Pas de droit sans technologie,* Bruxelles, Larcier, 2015, pp. 252 à 277.
- FRANCILLON, J., « Cybercriminalité. Aspects de droit pénal international. – La société de l'information et le droit pénal », Actes du colloque préparatoire de Helsinki du 10-12 juin 2013 organisé par l'Association Internationale de Droit Pénal, *Revue Internationale de Droit pénal,* 2013, pp. 1 à 38.
- FRYDMAN, B., « Les formes de l'analogie », *Analogie et méthodologie juridique*, Cahiers de méthodologie juridique n° 10, *Revue de la Recherche Juridique - Droit Prospectif*, Presses Universitaires d'Aix-Marseille, 1995, pp. 1053 à 1064. Disponible sur : http://www.philodroit.be/Les-formes-de-l-analogie
- GIACOMETTI, M. et MONVILLE, P., « Réseaux sociaux, anonymat et faux profils : vrais problèmes en droit pénal et de la procédure pénale », *Les réseaux sociaux et le droit »*, sous la direction de M. SALMON, Bruxelles, Larcier, 2014, pp. 179 à 210.
- INCALZA, T., « Strafonderzoek in het digitale tijdperk : zoeking en inbeslagneming », *Jura Falc.*, 2010-2011, vol. 2, pp. 329 à 383.
- KERKHOFS, J. et VAN LINTHOUT, PH., « Inleiding tot he materieel en strafprocedureel cyberstrafrecht: uitdagingen voor de advocatuur », *Internet &/@ Recht,* sous la direction de B. DE MEULENAERE, Gent, Larcier, 2013, pp. 5 à 44.

- KERKHOFS, J. et VAN LINTHOUT, PH., « Cybercriminaliteit doorgelicht », *T. Strafr.*, 2010, n° 4, pp. 179 à 199.
- KEUSTERMANS, J. et DE MAERE, T., « Tien jaar wet informaticacriminaliteit », *R.W.*, 2010-2011, n° 14, pp. 562 à 568.
- KUTY, F., *Principes généraux du droit pénal belge,* tome 1, Bruxelles, Larcier, 2009.
- LEROUX, O., « Arnaques, fraudes et escroqueries sur internet : moyens concrets d'investigation. Point sur l'affaire dite *Yahoo !* à la suite du second arrêt de la Cour de cassation », *J.T.*, 2012, pp. 839 à 843.
- LEROUX, O., « Criminalité informatique », *Infractions contre les biens,* sous la direction de H.-D. BOSLY et CH. DE VALKENEER, Bruxelles, Larcier, 2008, pp. 365 à 453.
- LEROUX, O., « Le faux en informatique », *J.T.*, 2004, n°6140, pp. 509 à 520.
- LEROUX, O., « Vers un premier faux informatique », obs. sous Civ. Liège (12e ch. corr.), 18 novembre 2002, *R.D.T.I.*, 2003, pp. 95 à 103.
- MAPLE, C. ET LANG, R., « Vulnerability, victims and free movement : the case of cyberstalking », *New Journal of European Criminal Law,* 2012, vol. 3, pp. 208 à 221.
- MEUNIER, CH., « 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, pp. 611 à 688.
- NIHOUL, M., « A propos de la précision requise pour définir une infraction en vertu du principe de légalité ou de prévisibilité du droit pénal », *J.T.*, 2004, pp. 2 à 6.
- PUTZ, J.-L., « Observations », note sous Cour d'appel (5e ch.), 19 février 2013, *J.T.L.*, 2013, n°23, pp. 81 à 84.
- TULKENS, F., VAN DE KERCHOVE, M., CARTUYVELS Y., e.a., *Introduction au droit pénal. Aspects juridiques et criminologiques,* Bruxelles, Kluwer, 9e éd., 2010.
- VAN EECKE, P., *Criminaliteit in cyberspace*, Gent, Mys & Breersch, 1997.
- VERBIEST, T. et DERVAUX, J., « La criminalité informatique dans tous ses états », *TBH*, 2002, vol. 8, p. 60 cité dans T. INCALZA, « Strafonderzoek in het digitale tijdperk : zoeking en inbeslagneming », *Jura Falconis Jg.*, 2010-2011, vol. 2, p. 330.

JURISPRUDENCE

- Cour eur. D.H., arrêt Matei c. France, 19 décembre 2006, req. n° 34043/02.
- Cour eur. D.H., arrêt Radio France et autres c. France, 30 mars 2004, req. n° 53984/00.
- C.J.U.E. (grande chambre), 8 avril 2014, (Digital Rights Ireland Ltd, Kärntner Landesregierung, e.a.), C-293/12 et C-594/12, disponible sur : http://curia.europa.eu/.
- Cass., 4 septembre 2012, inédit, cité dans O. LEROUX, « Arnaques, fraudes et escroqueries sur internet : moyens concrets d'investigation. Point sur l'affaire dite Yahoo ! à la suite du second arrêt de la Cour de cassation », *J.T.*, 2012, p. 842.
- Cass., 18 janvier 2011, *T. Strafr*., 2011, vol. 2., p. 120.
- Cass., 5 janvier 2011, *R.D.P.C.*, 2011, pp. 583 à 589.
- Cass., 29 juin 2005, *Pas.*, 2005, p. 1470.
- Cass., 30 novembre 2004, cité dans J. DEENE, « Illegaal kopiëren is geen diefstal », *Juristenkrant,* 2005, n° 102, p. 11.
- Cass., 2 octobre 2002, *Pas.*, 2002, p. 1796.
- Cass., 23 décembre 1998, *J.L.M.B.*, 1999, p. 393.
- Cass., 23 septembre 1981, *Pas.*, 1982, p. 123.
- C.C., 11 juin 2015, n° 84/2015.
- C.A., 30 janvier 1999, *Rev. dr. pén. crim.*, 1999, p. 808
- Anvers, 20 novembre 2013, *T.Strafr*., 2014, p. 75.
- Bruxelles, 12 octobre 2011, *A&M*, 2012, vol. 2-3, p. 238 cité dans DE SCHEPPER, K., en VERBRUGGEN, F., « Ontsnappen *space invaders* aan onze *pacmannen?* De materiële en formele strafrechtsmacht van België bij strafbare weigering van medewerking door elektronische dienstverleners », *T. Strafr.*, 2013, vol. 3, p. 146.
- Gand, 30 juin 2010, *T. Strafr.*, 2011, vol. 2, p. 132.
- Bruxelles, 24 juin 1991, *R.D.P.C.*, 1992, p. 340.

- Liège, 25 avril 1991, *R.D.P.*, 1991, p. 1031.
- Corr. Termonde, 2 mars 2009, *T. Strafr.*, 2009, vol. 2, p. 116.
- Corr. Hasselt, 21 janvier 2004, *Computerr.*, 2004, liv. 3, p. 130.
- Civ. Liège (12e ch. corr.), 18 novembre 2002, *R.D.T.I.*, 2003, pp. 95 à 97.
- Corr. Gand, 11 décembre 2000, *Computerr.*, 2001, vol. 2, pp. 84 à 89.
- Corr. Bruxelles, 8 novembre 1990, *J.T.*, 1990, p. 11.
- Corr. Verviers, 4 octobre 1989, *J.L.M.B.*, 1990, p. 709.
- Cour de Cassation luxembourgeoise, 3 avril 2014, n°17/2014, *DAOR*, n° 111, 2014, pp. 156 à 166.

DIVERS

Rapports

- Rapport de *McAfee*, « Net losses: Estimating the Global Cost of Cybercrime. Economic impact of cybercrime II », Center for Strategic and International Studies, 2014, disponible sur : http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.
- Rapport de *Norton by Symantec*, 2011, disponible sur : http://be.norton.com/cybercrimereport.
- Union Internationale des Télécommunications, *Comprendre la Cybercriminalité : guide pour les pays en développement*, UIT, Genève, 2009.
- Conseil de l'Europe, *Criminalité organisée en Europe : la menace de la cybercriminalité*, Rapport de situation 2004, Editions du Conseil de l'Europe, 2006.

Sites web

- Site web regroupant les conventions du Conseil de l'Europe, http://www.conventions.coe.int/treaty.
- Site web de l'O.C.D.E, http://www.oecd.org/fr.

- Site web de l'Union Internationale des Télécommunications, http://www.itu.int.
- Site web du G8, http://G8.utoronot.ca/summit/index.htm.
- Site web de la banque mondiale, http://www.donnees.banquemondiale.org.
- Site web de la police fédérale belge, http://police.be/fed/fr.

Statistiques

- Statistiques sur l'accès à Internet dans les ménages belges, StatBel, disponibles sur : http://StatBel.fgov.be/fr/statistiques/chiffres/travailvie/tic.
  Egalement disponible dans les documents en annexe – n° 6
- Statistiques sur l'accès à Internet dans les ménages européens, EuroStat, disponibles sur : http://www.ec.europa.eu/eurostat/statistics-explained.
  Egalement disponible dans les documents en annexe – n°7
- Statistiques du ministère public en matière de criminalité informatique spécifique, disponibles sur : http://www.om-mp.be/stat/.
  Egalement disponible dans les documents en annexe – n° 3, 4, 5, 9.
- Rapport de statistiques sur le développement des télécommunications dans le monde et base de données de l'Union internationale des télécommunications et estimations de la Banque mondiale, disponible sur http://donnees.banquemondiale.org/indicateur/.

Articles de presse

- DEPLA, T., « Politie registreerde 3,7% minder criminele feiten in 2014 », 15 juillet 2015, disponible sur: http://www.polinfo.be.
- MUNSTER, J.-F., « L'accès à nos donnes sera mieux encadré », Le Soir, mardi 4 août 2015.
  Egalement disponible dans les documents en annexe – n° 10.
- Rédaction en ligne, « Skype devant la justice à Malines, l'entreprise se pourvoit en cassation », 10 juin 2015, disponible sur : http://www.lesoir.be.

Autres

- Plan national de sécurité 2012-2015, disponible sur : http://www.police.be/files/fed/files/ORG/INT/PNS2012-2015.pdf.

- VERHAEGHE, K., « Opsporing en vervolging in cyberspace », mémoire de master en droit, Université de Gand, 2011-2012

- Lignes directrices de l'O.C.D.E. régissant la sécurité des systèmes et réseaux d'information – vers une culture de la sécurité, du 26 novembre 1992, C(92)188, Organisation de Coopération et de Développement Économiques.

- Rapport explicatif au premier protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, disponible sur : http://conventions.coe.int/Treaty/FR/Reports/Html/189.htm.

ANNEXES

Annexe 1. Entretien avec Koen Smets, inspecteur principal au FCCU et Marjolein Delplace, analyste stratégique au FCCU.

Recueilli par Caroline Heymans le lundi 27 juillet 2015 dans les bureaux de la police fédérale à Bruxelles, en langue néerlandaise.

Question 1. Kunt u zich allebei voorstellen en uw functie bij de FCCU uitleggen?

Marjolein Delplace: Ik ben Marjolein Delplace. Ik werk hier als strategische analist sinds 2006. Ik ben geen politie, maar wel burgerpersoneel binnen de politie. Ik ben dus geen operationeel lid van de politie maar burgerpersoneel van opleiding criminologe. Ik geef beleidsondersteuning en ik ben een beetje de persoon van de statistieken. En ook rapporteer ik over trends en evoluties in *cybercrime*. En ook bijvoorbeeld de vierjaarlijkse voorbereiding van het nationaal politieel veiligheidsbeeld dat de *input* is voor het nationaal veiligheidsplan.

Koen Smets: Ik ben Koen Smets. Ik ben operationeel dus ik ben een politieman. Het is mijn derde jaar op het FCCU. Ik ben hoofdinspecteur bijzondere specialisatie. Dus vijf jaar geleden werkte ik nog in het privé. Hier ben ik zowel operationeel als jurist. Ik noem mezelf operationeel jurist. Ik ben niet bezig met het nalezen van contracten en dit soort zaken, maar wel met de zaken die echt in verband zijn met *cybercrime*.

Question 2. Vindt u dat het Belgisch materieel strafrecht voldoende aangepast is om de verschillende infracties te straffen, die u op het internet ontmoet? Zijn er, volgens u, voldoende incriminaties in het strafwetboek om alle inbreuken die voorkomen op het internet aan te pakken? Zijn er volgens u bepaalde gedragingen die nog steeds ongestraft zijn omdat er geen adequate wetgeving is?

K.S.: Ik denk dat het wettelijk kader dat we hebben ruim genoeg is om aan te pakken wat er aangepakt moet worden. Met die technologie neutrale wetgeving zitten we effectief met een goed juridisch kader.

Het probleem is dat niet alles vervolgd kan worden en dat is eerder een beleidskwestie. Soms is het een frustratie dat bepaalde zaken niet vervolgd worden. De reden daarvoor is dat ze nu eenmaal niet moeten vervolgd worden, niet kunnen vervolgd worden of geseponeerd worden.

Maar in het kader zelf, tot nader orden, heb ik nog niets gevonden dat ik graag bestraft zou zien maar dat het niet kan omdat de wet niet ruim genoeg is. We zitten met zeer creatieve juristen aan onze kant van het openbaar ministerie enzovoort die genoeg fantasie hebben om de wet te interpreteren op die manier dat het toch bestraft wordt. Dus denk ik dat het wettelijk kader tot nader orde ruim genoeg is om alles aan te pakken. We kunnen dankzij de technologie neutrale terminologie heel veel beginnen interpreteren en dat geeft ons een heel stevig arsenaal aan middelen.

Question 3. Vindt u dat de BOM-wetgeving een rem is voor het werk dat de FCCU uitvoert op het internet? En bent u van mening dat infiltratie gemakkelijker gemaakt zou moeten worden op het internet?

K.S.: Ik spreek mijn eigen mening uit en ga hier niet in de naam van de FCCU of de politie spreken.

Ik zit in de *cybercrime* commissie waar we de wetgeving over *cybercrime* bespreken enzovoort. Er wordt daar nu net besproken over infiltratie op het internet lichter te maken tegenover het zwaar regime die de BOM-wetgeving oplegt. Ik vind dat dit persoonlijk een goede zaak zou zijn. De garanties die de BOM-wetgeving biedt in de reële wereld en die ook nodig zijn, moeten alleen maar verlicht worden. We zijn allemaal wel bewust van het belang van *privacy*. Dus het is niet dat we zeggen dat hier *privacy* en fundamentele vrijheden opgegeven moeten worden maar op het internet *nobody knows you are a dog*[311] en kun je zo gemakkelijk dingen aanbieden. En de burgerij of de misdadigers kunnen zoveel doen en als wij met het strenge regime van de BOM-wetgeving moeten handelen op het internet wordt het hopeloos. Dus ik ben van mening, ten persoonlijke titel, dat infiltratie gemakkelijker mag gemaakt worden, met de nodige *checks en balances*. Het is zeker dat ik er niet voor ben om te zeggen "doe maar alsof dat je Napoleon Bonaparte bent en doe maar alsof dat je drugs wilt kopen", daar ben ik helemaal niet voor. Maar het moet lichter.

[311] Référence au célèbre dessin de presse de Peter Steiner pour le New Yorker le 5 juillet 1993.

De BOM-wetgeving is een heel zware wetgeving. Als we het minder streng maken, kunnen we ook de hoeveelheid kleine misdaden dat je op het internet tegenkomt effectiever bestrijden door bijvoorbeeld lokale zones alle zoekertjes laten nagaan. Daarmee bedoel ik dat als er bijvoorbeeld een camion *iPads* gestolen is, we zouden kunnen na gaan op *EBay* wie er ineens kilo's *iPads* aanbiedt. Dit is geen zware infiltratie. Maar met de BOM-wetgeving zijn we dan vertrokken met procedures en verslagen. Dus infiltratie zou moeten gemakkelijker gemaakt worden. Absoluut.

Question 4. Hoe verloopt een onderzoek concreet na een klacht, een melding op E-cops of het vinden van een inbreuk?

M.D.: *E-cops* is sinds 17 juli 2015 niet meer operationeel. Dus de *website* bevat nu een doorverwijzing naar andere *websites*. *E-cops* is een beetje uitgegroeid tot iets wat onbeheersbaar was geworden en eigenlijk vaak ook mis-begrepen werd door de burger en ook door de politie.

De bedoeling van *E-cops* was gewoon om melding te maken van iets dat men had gezien op het internet. Bijvoorbeeld kinderpornografie of een *phishing* site mocht men op *E-cops* melden. Maar het werd meer en meer gebruikt door de burger om zich als slachtoffer te melden terwijl er op *E-cops* geen klacht kan worden ingediend. Het diende alleen voor meldingen. We moesten elke keer de burger doorverwijzen naar andere polities zoals de lokale zone. Op die manier had het *E-cops* meldpunt zijn doel voorbij geschoten.

Het was ook een kwestie van prioriteiten. De FCCU heeft minder en minder personeel en we zijn ons meer gaan focussen op de prioriteit *cybercrime* in strikte zin volgens de WIC[312]. De meldingen op het *E-cops loket* waren meer en meer traditionele misdrijven zoals oplichtingen en ook andere misdrijven waar we geen focus oplegden waardoor het eigenlijk zijn doel voorbij schoot. Het werd voor ons ook een heel zware last omdat je voor al die meldingen – 80 tot 100 meldingen per dag – de burger moest doorverwijzen. Het was onbeheersbaar geworden. Bovendien stuurden we in de meeste gevallen de burger van het kastje naar de muur sturen[313] om te zeggen "bedankt voor uw melding

[312] WIC est l'acronyme utilisé pour « Wet inzake informaticacriminaliteit » et fait référence à la loi du 28 novembre 2000 relative à la criminalité informatique, *M.B.*, 3 février 2001.
[313] Expression néerlandaise signifiant renvoyer sans cesse la personne d'un endroit à l'autre.

maar u moet naar uw lokale politie gaan". Dus daarom is het *E-cops* meldpunt eigenlijk afgesloten.

Kinderpornografie is nu een uitzondering die nog gemeld kan worden, bij *Child Focus* en *Child Focus* stuurt de meldingen door aan de politie dus die komen dan toch nog bij ons binnen. Ook voor economische wetgeving hebben we een link gezet naar FOD Economie om het te melden. Maar voor andere misdrijven verwijzen we door naar de lokale politie. Op de website kan je je postcode intikken en krijg je het adres van de lokale politie.

Wat het concreet onderzoek betreft, ofwel is er klacht van een burger ofwel in de dossiers bij ons wordt er informatie aangeleverd. Maar het zoeken van een inbreuk doen wij eigenlijk niet veel.

K.S.: Als we op een kinderporno *website* of zoiets stoten, dan melden wij dat wel maar we starten meestal van een klacht. Een burger komt een klacht indienen en we acteren die klacht. We zijn de FCCU dus wij zijn derde lijnsupport. We komen zelden in contact met de burger zelf. Meestal is het de RCCU die de klacht acteert en dan gaat dat naar de procureur. Die procureur leest en stuurt een kantschrift voor de zaken die we moeten doen. Bijvoorbeeld een burger die klacht komt indienen om te zeggen dat zijn pc ge*hacked* is zal het openbaar ministerie ons waarschijnlijk bevelen sturen in het genre "gaat die pc eens analyseren om te zien of die ge*hacked* is of niet". Zo nemen we het voorwerp van die burger om te zien wat er gebeurt is. We nemen dus een forensische kopie van die pc. We gaan na of die pc ge*hacked* is. Als die pc ge*hacked* is, gaan we op zoek naar bewijzen. Acteren we dat in een pv. Het gaat weer naar het openbaar ministerie. Het openbaar ministerie gaat waarschijnlijk zeggen dat we moeten onderzoeken naar verdere sporen. Vinden we IP-nummers en die moeten we dan identificeren. Dat soort zaken. Het is een vrij standaard procedure van wisselwerking tussen de politie en het openbaar ministerie en in geval dat het nodig is kan de onderzoeksrechter erbij betrokken worden bijvoorbeeld als er fundamentele vrijheden worden geschonden of huiszoekingen moeten gebeuren. We zoeken een beetje alles uit en op het einde beslist het openbaar ministerie of ze wel of niet gaan vervolgen.

M.D.: Specifiek voor FCCU – en niet voor RCCU of lokale politie – is dat we informatie krijgen aangereikt door bepaalde partners. Ze zeggen ons bijvoorbeeld dat dit of dit IP-adres geïnfecteerd is en dan doen wij het omgekeerde richting uitgaan. We overleggen

dan met het federaal parket en gaan dan de slachtoffers identificeren en op de hoogte brengen en kijken hoe het verder gaat met het federaal parket.

K.S.: Ja we krijgen deze informatie door "bevriende partners". We noemen dit "bevriende partners" maar wettelijk zijn ze meer met informanten-werk bezig. Die signaleren dan effectief als ze iets raars ontdekken en dan doen we de omgekeerde weg.

Ik wens niet antwoorden op de vraag of dit vaak gebeurt. Een voorbeeld werd uitgesmeerd in de pers, dus kan ik dit wel gebruiken: de *Belgacom*-affaire. We kregen ergens te horen dat dit en dat en dan zijn we met het federaal parket begonnen werken.

Question 5. Hoe gaat u om met het internationaal karakter van sommige inbreuken? Werkt het FCCU samen met andere *Computer Crime Units*? Werkt dit effectief? Is dit systematisch? Welke zijn de grootste moeilijkheden die u op dit vlak ondervindt?

K.S.: *Cybercrime* is bijna de facto internationaal. Dus er wordt vrij veel samengewerkt met andere *Cybercrime Units*. Informele samenwerking verloopt relatief vlot denk ik. We zijn bevriend met de meeste internationale politiediensten. Een keer dat we echt legaal moeten samen werken, dat gebeurt vrij systematisch.

Of het effectief is, wel het is een rompslomp van papier en dat soort zaken. Identificatie van een IP-adres in het buitenland zonder levensbedreigende situatie of bedreigen van kritische infrastructuur moet gebeuren door een rechtshulpverzoek. Dat kan meerdere maanden duren. Het kan zeker effectief werken. Er is zeker een wil tot samenwerking van alle internationale en nationale zaken maar de paperasserij maakt dat het traag gaat. Dit is eigenlijk de grootste moeilijkheid op dit vlak.

Met het *Cybercrime*-verdrag zijn er heel goede procedures het leven ingeroepen en heel handige zaken waar we gebruik van maken. Maar het probleem is dat we altijd via de hiërarchie moeten passeren en veel andere langzame stappen moeten volgen. Het neemt veel tijd in beslag. Dat is het grootste probleem met het transnationaal karakter. Er moet nog aan gewerkt worden. En er wordt er degelijk aan gewerkt om te zien hoe we de zaken kunnen bespoedigen.

We hebben met bepaalde nationale spelers zoals *Facebook* of *Microsoft* goede relaties. We werken al heel vlot mee samen. Ga het over levensbedreigende situaties of dreigingen tot aanslagen zoals het dreigen dat ze België gaan opblazen… dat soort zaken kunnen we binnen het uur antwoord krijgen op een bepaald *request*. We moeten dan

ook eerlijk zijn in die mate dat we niet om de vijf minuten kunnen schrijven dat een situatie levensbedreigend is. Als het een gewone zaak is dan pakt het zijn tijd maar voor andere zaken kunnen ze heel snel reageren. Maar het gaat hier wel over commerciële spelers. Het gaat hier niet over een bepaald land of een staat gaat. Met commerciële partners die transnationaal zijn, kan er snel samengewerkt worden maar met andere staten, dan kan het ook in die situaties zijn tijd nemen.

Question 5. Welke zijn de inbreuken die het meest voorkomen op het internet, zowel wat specifieke en niet-specifieke informatica misdrijven betreft?

M.D.*:* De inbreuken op het internet bevatten zowel de specifieke en niet-specifieke cybercriminaliteit dus is het hier een beetje moeilijk om te antwoorden omdat het niet op die manier wordt geregistreerd. Wordt geregistreerd op de klassieke manier bijvoorbeeld oplichting, kinderpornografie etc. en dan is er een specifieke categorie voor de echte informaticacriminaliteit.

Voor de niet-specifieke cybercriminaliteit is het aspect informatica iets extra die wel genoteerd is in het P.V. dat er gebruik werd gemaakt van ICT maar dat wordt niet geregistreerd in de statistieken. Daarom is het heel moeilijk om daar een antwoord op te geven. En het aspect internet duikt bij alle fenomenen ondertussen op: van wapenhandel tot drugshandel etc. Alles gebeurt nu op het internet met een grotere rol voor het *Dark-Net*.

En dan specifiek voor informaticacriminaliteit blijft het eigenlijk moeilijk want het is geregistreerd volgens de strafrechtelijke inbreuk dus ofwel *hacking*, informaticasabotage, informaticabedrog of informaticavalsheid.

Maar vaak zijn er verschillende inbreuken te registreren. Je hebt dus eigenlijk geregeld een dubbele registratie die gebeurt. Want een zaak kan bijvoorbeeld *hacking* en informaticabedrog zijn. Meestal wordt informaticabedrog geregistreerd omdat die inbreuk met de zwaarste gerechtelijke gevolgen heeft. Dus is het moeilijk een antwoord te geven op de vraag.

En wat het type van informaticacriminaliteit die het meest aan bod komt betreft, ik noem dat de "gelegenheid *hacking*". Puur kwantitatief gezien, komt dat het meest voor in de statistieken. Het is de niet professionele *hacking*. Het is de *hacking* van bijvoorbeeld de *e-mailaccount* van een ex-vriendje hacken of een vals *Facebook* maken van een persoon

etc. Dus eigenlijk heel veel van die feiten die geregistreerd worden door het openbaar ministerie of de politie gaan over dat soort *hacking*. Maar dat is eigenlijk de amateur en minder belangrijke feiten. Kwantitatief is dat het overwicht maar kwalitatief is dat eigenlijk de minder belangrijke criminaliteit. Maar de zwaardere dossiers zoals *hacking* van bedrijven, *hacking* van overheden, *hacking* van publieke figuren, … zijn belangrijker, maar komen minder voor. Er is een groot verschil tussen kwantiteit en kwaliteit in wat de geregistreerde criminaliteit betreft.

Question 6. Is er sprake van een strafrechtelijk beleid wat betreft informaticacriminaliteit?

K.S.: De FCCU houdt zich niet bezig met de kleine criminaliteit zoals bijvoorbeeld die valse erfenis die je zal krijgen als je 500 dollar stort. Dat is een kwestie van beleid. Dat is door het beleid opgelegd. Er is dus een beleid. Wij hebben daar geen inspraak over. Zij beslissen wat naar de FCCU gaat, wat naar de RCCU gaat en wat naar de lokale politie gaat. Het is soms een beetje moeilijk om te weten wie zich met welke zaken bezig houdt.

M.D.: De FCCU doet alleen zelf/autonoom dossiers als er echt kritieke infrastructuur aan te pas komt, dus eigenlijk de grotere zaken. En in andere zaken kunnen we dus steun geven aan de RCCU als ze zitten te werken met complexe netwerken of zo iets, dan geven we steun. De RCCU houden zich bezig met bijvoorbeeld informaticacriminaliteit die iets met bedrijven te maken heeft. De lokale politie houdt zich bezig met de gelegenheids-informaticacriminaliteit. Dat is *grosso modo* verdeeld maar dat wordt binnenkort wat meer uitgeschreven met de optimalisatie van de politie. Bijvoorbeeld gaan de RCCU van de hoven van beroep en grotere rol krijgen en dus dat is iets dat nu nog niet expliciet op papier ligt maar we zijn eraan aan het werken.

Question 7. Vindt u dat de FCCU over voldoende middelen beschikt om cybercriminaliteit effectief aan te pakken?

K.S.: Ik spreek hier weer uit eigen naam en niet in naam van de FCCU. Neen de FCCU heeft niet genoeg middelen. Bij uitbreiding de RCCU ook niet en de hele politie niet. Dat is een puur persoonlijk standpunt.

M.D.: Het FCCU telt nu 31 leden. Elk jaar daalt het een beetje. Mensen gaan weg en ze worden niet vervangen.

K.S: Die dat weggaan zouden normaalgezien vervangen moeten worden. Dat heeft dus niet te maken met geld. Het is een beetje van alles.

De overheid doet inspanningen om gespecialiseerd personeel aan te trekken. Het probleem is dat we zitten te dweilen met de kraan open[314]. Er is zoveel dat er gebeurt dat er nooit genoeg personeel zal zijn om alles op te lossen. De FCCU is onderbemand, de RCCU zijn onderbemand. De overheid is bezig aan inhaalbewegingen maar er zijn heel veel jaren die moeten ingehaald worden. Wat maakt dat het allemaal een beetje lijkt op een processie van Echternach[315].

We kunnen de overheid niet beschuldigen dat ze helemaal niets doen maar langs de andere kant kunnen we toch wel iets zeggen. Twee jaar geleden werd er 10 miljoen euro beloofd voor het *cybercrime* center en ze zijn het vergeten in te schrijven in de begroting. Dan krijgen we wel een licht gefrustreerd gevoel. We dachten dat we na *Belgacom* onze virtuele 9/11[316] hadden gekregen en dat de overheid wel zeer bewust zou zijn dat ze een tandje bij moeten steken. In de pers werd er veel gezegd dat de overheid begrijpt dat er een probleem is maar na een tijdje verdween het in de pers en daarmee verdween de focus op *cybercrime* en alle goede bedoelingen.

M.D.: FCCU behandelt niet alleen cybercriminaliteit in strikte zin maar we geven ook forensische steun dus analyse van ICT materiaal in andere dossiers. Dat neemt dus ook een stuk van onze capaciteit maar als we afdalen naar de RCCUS neemt die forensische steun bijna alle capaciteit in beslag, waardoor er bijna geen tijd meer is voor de *cybercrime*. Ondertussen bij bijna alle misdrijven is er een computer of telefoon die geanalyseerd moet worden. Ze zitten dus met veel achterstand. Het blijft binnenkomen en er is bij hen bijna geen tijd meer voor *cybercrime*. 90% van hun tijd gaat naar die forensische steun. Bij ons, op de FCCU, is er nog een sectie apart gehouden voor die *cybercrime* maar bij hen is het onmogelijk. Dus dit is een belangrijke opmerking.

[314] Expression néerlandaise qui signifie littéralement « être entrain de torchonner avec le robinet ouvert ». Cette expression est utilisée afin d'expliquer que l'on lutte contre les symptômes sans s'attaquer à la cause du problème. Dans le cas présent, l'inspecteur souhaite signifier que le gouvernement fait son possible pour doter la police de quelques moyens supérieurs, mais qu'il n'y aura en quelque sorte jamais assez de moyens pour lutter contre le fléau qu'est la cybercriminalité.

[315] Expression néerlandaise faisant référence aux processions dansantes d'Echternach ou les participants font trois pas en avant et deux pas en arrière. Cette expression est utilisée afin de signaler que l'on avance mais à une cadence très lente.

[316] Référence aux attentats du 11 septembre 2001. Expression utilisée afin de signifier l'impact qu'a eu l'affaire *Belgacom* en Belgique.

K.S.: Stel bijvoorbeeld een pedo-dossier die heel gemakkelijk is want de prentjes op een desktop zitten en heel gemakkelijk kennis ervan kunt nemen, dan nog ben je 3-4 dagen bezig met het uitzoeken van waar die beeldjes van komen, beschrijven hoe men ze vond etc. Dat neemt dus heel veel tijd. Een simpele analyse van een pc en we zijn al 3 dagen kwijt en vaak gaat het over meer dan één pc, en ook nog USB-stickjes met meer data.

Er was een tijd dat 640 Kilobytes meer dan genoeg was voor een computer gebruiker maar nu heeft bijna elke computer gebruiker meerdere Terabytes. We moeten goed beseffen dat het heel veel tijd in beslag neemt om dit te kopiëren. De hoeveelheid data neemt exponentieel toe. Elk onderzoek krijgt men een explosie van data die we moeten analyseren.

Als we alleen *à charge* werkten, dan zou dit niet zozeer een probleem zijn. Maar we werken ook *à décharge* en dus moeten we alles analyseren. Bijvoorbeeld in een pedo-dossier moeten we voor elk prentje nagaan of hij het heeft gedaan, of hij het heeft ge*download*. Als hij dan zegt er zit een virus op mijn computer, ik heb dat niet gedaan, dan zitten we nog eens met uren analyses bezig.

We zijn relatief goed uitgerust om alles aan te pakken maar qua mankracht is er echt een tekort. En ook qua gerief zouden we ook een *update* mogen krijgen. En de *clouds* brengen ook problemen met zich mee. We zouden ten minste een verdubbeling of drievoudiging van het personeel nodig hebben.

Question 8. Ziet u doorheen de jaren een vermeerdering of een verandering van type in de Belgische cybercriminaliteit? Welke zijn volgens u de factoren die dit beïnvloeden? Gaat deze tendentie zich voortzetten in de volgende jaren?

M.D.*:* Dus sinds 2001 kunnen we de cybercriminaliteit gevat worden in de politie databank. Sinds dat jaar gaat het elk jaar omhoog. Elk jaar zijn er meer en meer feiten. Er was een piek in 2012 die der uitsprong. Het was te leiden aan de golf van *police ransomware*. Het was een blokkering van uw computer zogenaamd in de naam van de politie. Dit is de politie u hebt iets illegaal gedaan en u moet op dit nummer en "boete" betalen van 100 euro. Er was van dit type criminaliteit echt een piek, maar niet alleen in België maar ook in andere landen. Daarom lijkt het dat er in 2013 eigenlijk een daling

was. Maar die piek in de criminaliteitscijfers buiten beschouwing gelaten, gaat de stijging eigenlijk verder.

Er is ook een verandering van type. Er is een toename van zwaardere dossiers. APT-dossiers dus *Advanced Persistent Threats*. Het zijn eigenlijk meer gesofisticeerde *malware* die wordt gedetecteerd op bepaalde bedrijven. Dus zo een spionage op lange termijn van bedrijven of overheden. *Belgacom* is daar een goed voorbeeld van. Er is ook een toename van *banking*fraude en van de manieren waarop dit wordt gepleegd. Vroeger was dat ook met *malware* en virussen. Dan is er een piek geweest via *phishing* en via de telefoon ook. En nu in 2015 hebben we een nieuw virus, de Dridex-*malware*. De gebruikers van het Isabel-systeem gebruiken dat als *e-banking* toepassing. En sommige van die gebruikers zijn geïnfecteerd waardoor de bedragen veel groter zijn. *Online banking* is altijd met nieuwe modi. Er is ook en toename van de digitale afpersing. Dus bijvoorbeeld de *police ransomware*, nu is er de *cryptoransomware* dus een virus die uw gegevens versleutelt en je moet betalen om ze terug te krijgen. Of ook, meer openlijke afpersing. Bijvoorbeeld "Ik ben hacker X en ik heb u data ge*hacked*. Als je me niet betaalt dan ga ik die publiceren". Rex Mundi is daar een belangrijke speler en ook de *copy cats*.

Wat de factoren betreft is er de toename van ICT-afhankelijkheid van de *targets* en de slachtoffers. De professionalisering van *cybercrime* is ook een factor. Je kunt een virus kopen en aanpassen. Er is echt een commercialisering van *cybercrime*. Volgens mij is ook de verwevenheid van alle *devices* een factor. Een telefoon is nu een mini-computer met private en professionele gegevens op een toestel, dus het maakt u eigenlijk kwetsbaarder voor *cybercrime*.

De tendentie gaat zich voortzetten, daar zijn we van overtuigd.

K.S.: Ja, zeker en vast gaat deze tendentie zich voortzetten. Vorige week nog was er een mooi voorbeeld. Een auto wordt ge*hacked*. Niet een stilstaande auto, maar in het midden tijdens zijn rit werd de auto ge*hacked* en "bam" alles valt stil. Dus ja we zijn er zeker van dat er van alles nog gaat voorkomen. Een ijskast of een *pacemaker* kan ook al gehackt worden. Het gaat ver.

In mijn pessimistische persoonlijke visie, zijn we alleen het tipje van de ijsberg aan het bestrijden. En dat is zelf al een *understatement* want we weten niet eens waar de ijsberg

ligt[317]. We zijn meer symptoombestrijding aan het doen, dan degelijke oorzaakbestrijding.

M.D.: Zelfs een vliegtuig kan ge*hacked* worden.

Europol heeft gezegd dat cybercriminaliteit gaat stijgen in bereik, in complexiteit, in aantal en in type aanvallen. Zij zien het ook niet heel rooskleurig.

K.S.: Ja er is zoals we gezegd hebben een commercialisering van *cybercrime* maar ook een professionalisering van *cybercrime*. Mensen hebben nog veel de neiging te denken dat *hackers* alleen maar 16-jarigen *geeks* zijn. Dis is niet zo. De georganiseerde criminaliteit zit al helemaal op de *cybercrime*. *Cybercrime* is volgens sommige rapporten al meer winstgevend dan de drugshandel. Dat gaat blijven.

Onze huizen zijn nu allemaal goed beveiligd met een stevige voordeur en alles wat nodig is maar ons virtueel huis zit nog helemaal wijd open. Er is nog veel werk aan de winkel.

Question 10. Als we naar de statistieken van het Openbaar Ministerie kijken, zijn er in mate van cybercriminaliteit heel wat zaken die zonder gevolg blijven. Is dit demotiverend voor de FCCU?

K.S.: Die statistieken gaan meer op voor de RCCU. De zaken die wij mee bezig zijn, worden niet zo snel geklasseerd. Maar we werken wel aan bepaalde zaken, wetend dat ze nooit vervolgd zullen worden voor een rechtbank. Het is een stuk demotiverend maar het is ook onze taak.

We weten dat het onze taak is om het misdrijf vast te stellen. En dat doen we ook. En we doen alle dingen die we moeten doen en die we kunnen doen en hebben we onze job gedaan.

Op het niveau van de RCCU kan ik me wel voorstellen dat het demotiverend is omdat het bij hun vaker gebeurt. Ze steken tijd in die en die zaken om dan te horen dat het bijna sowieso is geseponeerd.

M.D.: De grootste oorzaak van die zonder gevolgstellingen in de cijfers van het openbaar ministerie is omdat de dader niet gekend is. Vaak kunnen we bepaalde pisten volgen maar niet echt tot aan de dader. Maar ik denk dat uit elk onderzoek er wel iets

[317] L'inspecteur souhaite à travers cette image signifier qu'il y a encore beaucoup de travail à accomplir et qu'on ne peut pas imaginer l'ampleur de ce qui nous attend.

geleerd wordt dus denk ik dat je er sowieso iets van leert ook al geraak je niet tot de dader.

K.S.: Dit is heel positief en juist verwoord. In de praktijk is het ook zo. We bijten ons vast waar dat we kunnen. Bijvoorbeeld met *Belgacom* was het heel duidelijk dat het niet ging over een persoon maar over een mogendheid. Ondanks dat we een zeer liberale wetgeving hebben daaromtrent, kunnen we nog niet andere mogendheden voor een rechtbank dragen. Dat gaat nooit gebeuren. Tot werkten we zo ver mogelijk als het kon en dan is het aan de diplomatie, de politiek, … om zijn werk te doen. *Belgacom* was een zeer mooi leerproces.

Question 11. Denkt u dat de bevolking, de bedrijven, de politici en de wetgever er genoeg van bewust zijn dat cybercriminaliteit een echt probleem is? En hoe zou men dit nog kunnen verbeteren?

K.S.: Neen, ze zijn er helemaal niet van bewust. Het is soms stuitend hoezeer dat men zich niet bewust is van wat er allemaal gaande is. Ik krijg soms het gevoel dat politici meer denken aan stemmen voor de volgende verkiezingen dan het beleid voeren.

De dataretentie-richtlijn is vernietigd geweest. Als de situatie zo blijft kan de FCCU en de RCCU eigenlijk opdoeken. Dan zijn we technisch werkloos. We kunnen niet meer veel doen.

De *hype* van het moment is *privacy*. En hoe dat het verkocht is, is dat de politie aan de gegevens van iedereen kan, wat helemaal fout is want we moeten een vordering krijgen en dit en dat. De publieke opinie wordt, in mijn ogen, gemanipuleerd. We zijn *Big Brother* niet. Maar dat is waar de burgerij schrik voor heeft. En dan krijg je, zoals vandaag in de krant, artikelen over *Google* die alles weet over waar we zijn. Voor *Google* hebben we geen probleem om onze privacy op te geven, maar als het de politie is dan is het een probleem. Ik heb andere dingen te doen in mijn vrije tijd dan alles en iedereen te controleren.

De bevolking is er dus niet van bewust wat het probleem is en ik heb soms het gevoel dat ze soms op de verkeerde wijze wordt ingelicht over waarom bepaalde regels moeten bestaan. We hebben nood aan bewustwording. Maar ik heb het gevoel dat de politie niet zo snel naar buiten komt om een maatschappelijk probleem aan te kaarten. Terecht misschien, want het is onze taak niet *per se*. De magistratuur komt ook niet naar buiten

om zo'n probleem aan te kaarten. De politiek die zijn meer bezig met de volgende verkiezingen dan met het voeren van het beleid, in mijn persoonlijke opinie. Dus iedereen schuift de zwarte piet toe[318] maar niemand doet iets.

Als die dataretentie compleet geannuleerd wordt, dan zullen we een alternatief moeten zoeken maar het enige alternatief is dat we veel meer huiszoekingen gaan moeten doen en tappen. Wat, volgens mij, een veel grotere inbreuk is op de privacy. Ze zijn er niet genoeg van bewust en we kunnen het verbeteren met een juiste communicatie en voorlichting naar de bevolking toe. Wie dat gaat doen dat weet ik niet.

M.D.: Het is een beetje contradictorisch want de vorige regering onder Di Rupo die had dan opgedragen om de cyberstrategie te schrijven. Dit werd gedaan maar dan moest er een centrum worden opgericht maar het budget dat werd goedgekeurd bleef dan hangen. Uiteindelijk is het opgericht en moest er dan selecties worden uitgevoerd. Dus dat duurt allemaal heel lang.

En nu ook in het regeerakkoord van Charles Michel stond dat ze onderzoekseenheden versterken voor de bestrijden van *cybercrime* maar concreet hebben we daar nog niets van gezien. Dus de politici, ook al klinkt het wat hard, doen alsof ze ermee bezig zijn, maar we zien niets. Misschien komt het nog maar waarom duurt het dan zolang, want het is iets dat eigenlijk heel dringend is.

En ook de burger, ik denk dat het voor veel mensen het nog ver van hun bed ligt[319]. Er is nog veel werk aan de winkel[320] is in mate van preventie.

Question 12. Bent u van mening dat als er een inbreuk is op een informaticasysteem dat niet beveiligd is, de verantwoordelijkheid gedeeltelijk bij het slachtoffer zou moeten liggen? Zou dit het bewustzijn van de bevolking stimuleren? Met andere woorden, zou een beveiliging van de informaticasystemen verplicht moeten worden?

K.S.: Een verplichte beveiliging van de informaticasystemen daar ben ik er echt voor. Het is een aberratie in onze wetgeving. Want als er een open netwerk is en je gaat erop, bam je bent bezig met *hacking*. Maar praktisch, feitelijk, elke persoon die iets illegaals wil doen kan zich op een onbeveiligd netwerk inloggen en we zijn vertrokken.

[318] Expression néerlandaise signifiant de transférer le problème à quelqu'un d'autre.
[319] Expression néerlandaise signifiant qu'il s'agit de quelque chose dont on ne se préoccupe pas (encore).
[320] Expression néerlandaise signifiant qu'il reste encore beaucoup à faire.

Iedereen zet een slot op zijn voordeur en we moeten ook naar beveiligde netwerken gaan. Anders als we een dader vinden die een open netwerk heeft gaat die sowieso zeggen dat die van niets weet en dat iemand op zijn netwerk heeft ingelogd.

Ook de systemen van netwerken mogen een betere *login* hebben maar dan zijn we weer bezig met dat *Big Brother* gedoe waar dat iedereen zoveel schrik voor heeft.

M.D.: Het nieuwe centrum *cybersecurity* gaat zich richten op het opstellen en verspreid toezien van standaard richtlijnen, veiligheidsnormen en ook certificatie van veiligheid van informatie- en communicatiesysteem maar dan vooral gericht op administraties en publieke instellingen. Dat is al absoluut het minimum. En dat er zelf nog een stap verder moet gegaan worden.

K.S.: In Duitsland is het alleszins verplicht om uw netwerk te beveiligen. En dat lijkt mij een simpele maatregel om te implementeren. Het is een pervers effect dat degenen die een open netwerk hebben meestal ook de meest kwetsbare groepen zijn, bijvoorbeeld grootouders.

Question 13. Er werd recent beslist dat de FCCU gedecentraliseerd zal worden. Wat zullen de gevolgen daarvan zijn? Denkt u dat dit invloed zal hebben op de efficiëntie van de FCCU?

M.D.: Het is nog niet definitief beslist. En nu waarschijnlijk zou het niet zo zijn, maar we weten niet veel meer[321].

K.S.: We weten niet wat het gaat worden. Afhankelijk van waar dat je staat, krijg je andere geruchten. Er is dus een onzekerheid en dat heeft op zich al invloed op de efficiëntie van de FCCU maar we blijven gemotiveerd en efficiënt tegen de misdaad strijden.

Question 14. Ten slotte, denkt u aan een verbetering die plaats zou kunnen vinden om de effectiviteit van het speuren, vervolgen en sanctioneren van cybercriminelen te verbeteren?

[321] Marjolein DELPLACE me fit part le 8 août 2015 qu'une modification a eu lieu et qu'en attendant la décision fut prise que le FCCU ne sera pas décentralisé et gardera ainsi sa capacité de recherche autonome.

K.S.: Ik heb er een, maar weer is dit heel persoonlijk. Ik zou graag de recht op domheid verbieden. Ik wil daarmee zeggen dat de mensen op het internet alles geloven en ik zou het tof vinden om dit wettelijk af te dwingen.

Neen, maar nu een beetje serieuzer we moeten sensibiliseren. Als iets op het internet te mooi is om waar te zijn, dan is het misschien niet waar en daar moet men meer bewust van zijn.

En op ander vlak zou ik ook andere zaken willen verbeteren. Als heel wat rompslomp vermeden worden in onderzoeken dat zou tof zijn. Maar meestal is die rompslomp nodig voor de rechten van de verdediging en zo. Maar soms denk ik dat dit niet nodig is en ik wel zal bewijzen dat hij het gedaan heeft maar ja, gelukkig heeft de verdediging ook nog zijn rechten maar soms gaat het te traag.

Cryptografie sleutels afgeven of een centraal laten beheren zou volgens mij een enorme verbetering zijn. Cryptografie is een echt probleem. Het is zelfs meer dan een echt probleem. Cryptografie is nu al bekend bij de boeven maar als het zich nog meer gaat spreiden, wordt het onmogelijk voor ons. Dan komen we toe, dan weten we dat de informatie hier of daar zit, maar we kunnen er niet aan. Bijvoorbeeld in sommige gevallen zijn we zeker dat we kinderporno prentjes hebben gevonden maar ze zijn gecrypteerd, we kunnen er niet aan en we kunnen niet aan de sleutels geraken en dus daar stopt het onderzoek.

Als de burgerij zelf begint te crypteren wordt het een echt probleem. Het zou misschien niet een slecht ding zijn dat ze wat meer gaan crypteren, bijvoorbeeld hun bankgegevens en zo. Maar als we de sleutels niet hebben dan kunnen wij niet vooruit gaan in een onderzoek.

Praktisch is er nog veel dat kan verbeterd worden.

M.D.: Ik denk ook aan die sensibilisering dat elke gewone burger meer bewuster is en voorzichtiger zou zijn zodat veel zaken vermeden kunnen worden.

K.S.: Op het café roep je niet “ik ga op vakantie”, wel roept het dan ook niet op *Facebook*. Het is het paradijs voor de vrije gedachten maar er is ook de *dark-web* en dus de mensen moeten er meer van bewust worden. Sensibilisering is een *must*.

Annexe 2. Entretien avec Luc Beirens, ancien directeur de la FCCU.

Recueilli par Kevin Verhaege, le 18 avril 2012 et disponible sur : http://www.scriptiebank.be

"In welke mate is de Belgische wetgeving aangepast aan de realiteit?"

Als we naar het materieel strafrecht kijken denk ik dat we vrij veel zaken dekken. Natuurlijk zijn er hier en daar wat zaken die afhankelijk zijn van wat de wetgever zelf wil. In Frankrijk bijvoorbeeld, heb je happy slapping, of websites die filmpjes tonen van moorden. Dit heeft met *cybercrime* op zich niet zoveel te maken, maar dat zijn zaken die er toch in zekere zin aan verbonden zijn. Dat heeft dan betrekking op de randfenomenen, met Internet als publicatiemiddel. Onze mogelijkheden wat de opsporing betreft worden wel enigszins beperkt door de strenge regeling in de BOM-wet. De mogelijkheid om te infiltreren bestaat, maar is wel verbonden aan allerlei voorwaarden. Het probleem met de huidige BOM-wet en de opsporingsmethodes is dat men deze moet gaan rechtvaardigen, maar dan moet je wel elementen hebben. Vaak moet je dan wel reeds elementen kunnen vinden, vooraleer je kan overgaan tot toepassing van de bijzondere opsporingsmethoden. Bijvoorbeeld op chatkanalen meelezen of meeluisteren is toegestaan, maar zelf iets typen of zeggen niet, want dat is dan infiltratie. Als je dan op chats waar kinderen opzitten niet mag meedoen, kan je ook niet zien wie die kinderen eventueel wil benaderen. We zijn in dat opzicht wat gekortwiekt. We mogen eigenlijk niet heel veel. Begrijp me niet verkeerd, ik begrijp de beweegredenen waarom dit niet zomaar toegelaten is. We moeten in de opsporing de middelen gebruiken die wettelijk zijn voorzien, met inachtneming van de grondrechten, de privacy, de bescherming van de woning en de bescherming voorzien in de wet op de elektronische communicatie van 2005. Voor alles wat daar tegen ingaat moet je dus machtigingen krijgen van de onderzoeksrechter of de procureur.

"Hoe verloopt een onderzoek dan concreet? Wat is de rol van het ecops loket?"

Ecops is duidelijk maar een meldpunt, de meeste zaken, zoals gewone misdrijven starten bij een klacht, waarbij de onderzoeksrechter ons vertelt wat te doen. Ofwel komt er dus een klacht, ofwel starten we zelf als we iets opmerken. Ecops is natuurlijk één van de startpunten, maar blijft erg beperkt voor ons werk. Bijlagen 193 "Wat zijn de grootste hindernissen waar jullie mee te maken krijgen gedurende de opsporing?" Als je kijkt naar het rechtskader dan zit het grootste probleem in het internationaal aspect. Van de 100 dossiers gaan er zeker 95 zijn waarbij we de grens moeten oversteken. In de meeste gevallen zitten de dader en het slachtoffer niet in hetzelfde land, en in het geval dat dit wel zo is, zitten er vaak systemen tussen waarvan de

sporen leiden naar het buitenland. Je zit quasi onmiddellijk in een behoefte om sporen in het buitenland te gaan onderzoeken.

"Werken jullie dan samen met buitenlandse Computer Crime Units?"

Jazeker, wij hebben internationale samenwerking via instrumenten als rogatoire commissies. Maar ook recenter zijn er initiatieven voor joint-investigation teams waarbij informatie kan uitgewisseld worden van het ene dossier naar het andere. Het intermezzo waar we eigenlijk het meest mee werken zijn rechtshulpverzoeken. Maar het nadeel daaraan is dat het grote vertragingen meebrengt in het dossier en je kan niet vlot gaan uitwisselen met uw collega"s. Het is echter niet aan ons om te gaan kiezen met welke eenheid we gaan samenwerken, het is het land zelf dat bepaalt welke eenheid daar wordt opgezet. Het is wel zo dat er in elk land een 24u permanentiepunt aangeduid is. Als er zeer dringende gevallen zijn kunnen wij contact opnemen met zo"n permanentiepunt en dan wordt het dossier op die manier opgestart. In de meeste gevallen is dat opstarten het feit dat er gegevens bewaard worden ofwel dat we direct informatie geven, waardoor er in het land in kwestie ook een dossier gestart wordt. En dan is het aan de magistraten wat ze concreet kunnen gaan opzetten van samenwerking en welke gegevens het ene land nodig heeft van het andere.

"Met welke inbreuken krijgen jullie het vaakst te maken?"

Het is zo dat we domeinen afbakenen. Wij, als FCCU, maken deel uit van de directie financieel-economische criminaliteit. Normaal gezien, als autonome dienst, hebben wij geen autonome opsporingsbevoegdheid. Dat wil zeggen dat de mensen normaal bij de lokale politie gaan om een klacht neer te leggen, waarna een dossier wordt opgestart. De lokale politie gaat voor beperkte lokale misdrijven hun lokale recherche inschakelen. Eens dat dit arrondissement overstijgend is gaat dat naar de federale recherche. De federale gerechtelijke politie is dan weer op twee niveaus opgesplitst, waarbij de centrale diensten ondersteuning geven aan de arrondissementele diensten. Ofwel worden de dossiers gedraaid door de lokale politie, ofwel door arrondissementele diensten van de federale gerechtelijke politie, waarbij de centrale diensten maar in steun komen. Nu zijn er uitzonderingen op dat principe, en die zitten Bijlagen 194 allemaal in de directie financieel-economische misdrijven. Hier vertrekken we vanuit het principe, wettelijk voorzien, van de georganiseerde financiële criminaliteit. Daar is dus een speciale dienst binnen onze directie voor. Dan heb je ook nog de anti-corruptie dienst, en daarnaast dan de Federal Computer Crime Unit. Concreet wordt er tussen de federale politie en het FCCU afspraken gemaakt hoe we gaan samenwerken bij aanvallen op grote kritieke systemen. Als de federaal procureur beslist dat een dossier gedraaid wordt door het federaal

parket, als ze m.a.w. een zaak federaliseren, dan kan de federaal procureur de FCCU aanduiden als opsporende eenheid. Zo draaien we in feite wel een autonoom dossier, wat eigenlijk een uitzondering is op het wetgevend model. Dat is ook noodzakelijk gebleken, omdat je in dergelijke dossiers vaak met sporen zit in eigen land, verspreid over verschillende arrondissementen, maar eveneens met internationaal verspreide sporen. Bijkomend heb je dan het aspect van de specialisatie voor zo‟n complexe dossiers, die niet zo verspreid zit binnen de politie. We hebben dan wel 25 Regionale Computer Crime Units met specialisten, maar als je maar af en toe in contact komt met dergelijke vormen van criminaliteit dan heb je natuurlijk minder ervaring. Als ik dan spreek over de criminaliteit waar wij ons met de Federal Computer Crime Unit mee bezig houden, gaat dat over hacking van zeer grote bedrijven die deel uitmaken van de kritieke infrastructuur. Indien deze zouden platgelegd worden, dan krijg je economische problemen in het land. Dus telkens wanneer zo‟n dossier zich aanbiedt gaat de FCCU dat afchecken met het federaal parket, met de vraag of er wordt gefederaliseerd of indien er enkel wordt gecoördineerd. Ofwel behandelen we het dossier dan autonoom, ofwel geven we ondersteuning aan de mensen op het terrein. De vormen van cybercriminaliteit die het meest worden geregistreerd in de databanken van de politie zijn vooral misbruiken van kredietkaarten. Dat is de hoofdmoot van wat geregistreerd wordt. Daarnaast hebben we ook zaken die onder andere te maken hebben met hackingen van Internetaccounts, hotmail e.d.. We hebben echter maar een beperkt aantal gevallen per jaar van bedrijven die het slachtoffer worden van hacking en daar een klacht voor neerleggen. Zeer grote bedrijven zijn dan wel uitzonderlijk, toch hebben we enkele van die dossiers. In zulke gevallen zie je dan ook meteen het internationale aspect weer opduiken, waarbij we niet enkel in België onderzoeken moeten doen, maar ook moeten samenwerken met politiediensten uit andere landen, omdat die bedrijven multinationals zijn. Hun infrastructuur is dan ook verspreid over Europa, en zelfs wereldwijd. Wat wij in het recente verleden gedaan hebben, sinds 2007, was focussen op al wat e-banking misdrijven betreft. Het is dan niet zozeer de bank die hier slachtoffer van wordt, maar meer de eindgebruiker, waarbij cybercriminelen kunnen binnendringen tijdens de eigenlijke transactie. Het betreft dan bijvoorbeeld zaken omtrent phishing-websites, maar nog Bijlagen 195 voorkomend zijn de zaken waarbij de eindgebruiker wordt geïnfecteerd waardoor zijn pc in een botnet komt te staan. Dat botnet gaat dan instructies geven aan die pc‟s om bepaalde data te verzamelen. Op het moment dat de gebruiker naar zijn bankwebsite gaat, gaat hij een signaal geven naar de cybercrimineel in het botnet, dat de gebruiker naar de bankwebsite aan het gaan is. Terwijl de gebruiker dan naar de bankwebsite gaat, komt de crimineel over uw verbinding mee om zo transacties te doen. In België zijn we op dat punt nog vrij goed beveiligd, gezien de

cybercrimineel de medewerking van de gebruiker nodig heeft om een transactie te kunnen doen. Dan probeert men via allerhande trucs om de gebruiker zover te krijgen om de transactie effectief te bevestigen. Het paswoord en de gebruikersnaam heeft de cybercrimineel op dat moment reeds. Het enige dat hij nog nodig heeft is dat de gebruiker met zijn digipass de transactie bevestigt. Ofwel wordt je dan gebeld, ofwel worden bijkomende schermen gepubliceerd in uw connectie met de bank onder het mom van een securitytest. Alle dossiers die te maken hebben met deze problematiek worden door het FCCU behandeld. Recentelijk krijgen we ook vaker gevallen van ransomware, waarbij mensen hun pc geblokkeerd wordt en waarbij gezegd wordt dat ze een bepaald bedrag moeten betalen om de blokkering op te heffen. Een doorsnee hacking van een facebook profiel wordt niet op het niveau van de FCCU behandeld, tenzij dit te maken heeft met een persoon die een sleutelpositie vervult binnen zo‟n kritische infrastructuur. Als het bijvoorbeeld een systeembeheerder betreft, waarbij men informatie kan halen om toegang te krijgen tot die kritische infrastructuur, dan komen we wel in actie en beschouwen we dit als een deel van de hacking van de kritische infrastructuur zelf. “Hebt u zicht op de mate waarin deze zaken ook effectief worden gevolgd door een vervolging?” Bij die e-banking transacties liepen veel sporen naar het buitenland, daar hebben we inderdaad veel mensen kunnen identificeren, en zowel witwassers als hackers kunnen laten oppakken. Maar hier heb je dan ook weer direct dat internationaal aspect dat de kop opsteekt. Rusland gaat hun onderdanen niet uitleveren om ze hier te veroordelen en ze hier in de gevangenis te stoppen. Ze gaan die criminelen daar zelf berechten, in zoverre dat dit dan ook effectief gebeurt. We hebben in dit kader zeker al successen geboekt, al is dit niet zo duidelijk en zichtbaar als resultaat voor de Belgische justitie. Als wij immers uiteindelijk ons dossier overdragen aan die buitenlandse politiediensten, hopen wij dat zij verder het dossier afwerken en effectief iemand gaan aanhouden. Maar dat is spijtig genoeg niet telkens het geval. We hebben in bepaalde gevallen al de indruk gehad dat de vooruitgang eerder tegengehouden Bijlagen 196 werd. Ook in België hebben we al mensen geïdentificeerd en aangehouden maar het blijft wel, naar mijn gevoel, een domein dat beschouwd wordt als zijnde niet echt schadelijk voor de maatschappij. Nochtans zien we dat er meer en meer aanvallen zijn op bedrijven en organisaties.

“U bent sinds 2001 hoofd van de FCCU. Heeft u gedurende die elf jaar een evolutie vastgesteld in de manier waarop *cybercrime* zich manifesteert? Zijn de fenomenen talrijker geworden, en meer agressief?”

Het gegeven is veel complexer geworden, en ook agressiever. Het is zo dat hacking vroeger vaak intern geschiedde. Het betrof dan vaak medewerkers van een bedrijf die omwille van de

zwakheden in het systeem, wisten hoe ze dat systeem konden misbruiken. Wat we nu zien is dat die hackingen meer van externe aard zijn, en het aantal ervan in snel tempo stijgt. Zo‟n activiteit heb ik nog nooit ervaren. Wat we niet doen zijn defacements van websites, tenzij dit over kritieke infrastructuur gaat. Maar als je kijkt naar het aantal websites dat gedefaced is, op de website hashzone, dan is dat een enorm aantal, duizenden op jaarbasis. We hebben er ons een tijdje mee bezig gehouden om de overheidsdiensten en belangrijke organisaties op de hoogte te brengen dat ze gehacked waren. Het spijtige is dat men daar schijnbaar weinig belang aan hecht. We hebben voorbeelden gehad van steden waar we contact mee opnemen met de melding dat hun website is gehacked. In eerste instantie zijn die mensen verrast, maar ze ondernemen geen stappen voor een betere beveiliging, waardoor ze nog geen week later opnieuw gehacked zijn. Dat is uiterst frustrerend voor ons. Nadien hebben we dan ook beslist om dit links te laten liggen, en onze aandacht te vestigen op aanvallen op kritieke infrastructuren en te trachten de netwerken van de criminelen te destabiliseren. Dat laatste doen we vooral door servers aan te pakken die criminelen gebruiken. Dat is echter een taak die we niet alleen kunnen doen. Enerzijds, zit je weer met het internationaal aspect en, anderzijds, is er ook samenwerking nodig met de service providers. Idealiter zou iedereen meer een stuk verantwoordelijkheid moeten gaan opnemen. Op zich moeten we zeker evenveel belang hechten aan het creëren van een bewustzijn omtrent cybercriminaliteit, dan aan de bestrijding zelf. Als de eindgebruiker zich beter wapent dan zal de crimineel zijn spionagemogelijkheden verliezen, evenals zijn aanvalscapaciteit. Het is dan ook noodzakelijk dat de politie en de industrie zelf gaan samenwerken, en dat er in dit opzicht dan ook initiatieven worden genomen op wettelijk vlak, waarbij ook een verantwoordelijkheid wordt gelegd bij de eindgebruikers. Men heeft in het verleden met de wet van 13 juni 2005 betreffende de elektronische communicatie een ietwat fout signaal gegeven. In die zin dat Bijlagen 197 men de eindgebruiker als een zwakke schakel beschouwde, waar grote broer politie voor moest zorgen. Naar mijn mening is dat contraproductief. Als je met je wagen op de openbare weg rijdt moet je een rijbewijs halen en moet je auto door de keuring geraken. Als je op het Internet gaat daarentegen, moet je je van niets iets aantrekken. Mensen die zonder anti-virus werken, die zeer nonchalant zijn in hun keuze van wachtwoorden, geen firewall hebben of toch blijven verder werken ook al weten ze dat ze geïnfecteerd zijn, zoeken naar mijn mening problemen.

“Beschikt de FCCU over voldoende personeel en moderne middelen om *cybercrime* aan te pakken?”

Momenteel zijn er bij de FCCU 35 mensen aan het werk, waarvan 10 administratief personeel. Bij de 25 Regional Computer Crime Units (RCCU‟s) werken zo‟n 170 mensen, waarvan een

20-tal administratief personeel. Dit is niet echt voldoende, als je kijkt naar wat er verwacht wordt. Vooreerst is er het forensisch computeronderzoek in het kader van traditionele criminaliteit, zoals sociale fraude, drugs, en tegelijkertijd ook het behandelen van cybercriminaliteit. In dat opzicht is het aantal personeelsleden dan ook niet genoeg om te doen wat we moeten doen. Maar dat we met te weinig personeel kampen is een oud zeer. Op zich kan je dit enigszins beperken door in infrastructuur te investeren, waardoor je meer kan doen met minder mensen. Maar dan moeten die investeringen natuurlijk ook gebeuren, anders kom je met een structureel probleem te zitten, wat op dit moment het geval is. Reeds in 2006 werd er door de regering vooropgesteld dat er in 2011, 293 persoonsleden moesten zijn. Dat aantal is nooit bereikt, maar het markante aan de zaak is dat die berekening gebaseerd is op de behoeften die er destijds in 2006 waren. Ondertussen is de wereld compleet veranderd, en zijn die cijfers uit 2006 ook niet meer relevant. Vandaag loopt praktisch iedereen rond met een smartphone, tablets e.d.. Op de duur zit je met zoveel toestellen per gebruiker waarop inbreuken kunnen gebeuren, dat de wachtlijsten echt ellenlang worden. Ook wat budget betreft zijn we niet ruim bemeten. Het is altijd zoeken naar een werkbare oplossing, en wij passen ons aan, en doen onze best met wat we krijgen. Niettemin is wat we krijgen een minimum minimorum, als je vergelijkt welke budgetten er zijn in bijvoorbeeld Nederland, Noorwegen of Zweden. In vergelijking met die landen werken wij op minimalistische scenario‟s. Dit dient echter ook genuanceerd te worden; als je vergelijkt met een groot aantal andere landen, dan staan we er ook weer niet zo slecht voor. Bijlagen 198

“Kan de FCCU zich meten met Computer Crime Units uit het buitenland?”

Qua kennis en kunde die wij in huis hebben wil ik mij meten met gelijk welk ander land. Qua wettelijk kader en middelen is het natuurlijk een ander verhaal. Wat dat laatste betreft zijn we voor op de ene dienst, en ver achter op de andere. Als je kijkt naar wat er in Nederland geïnvesteerd wordt in vorming, dan kunnen wij niet anders dan jaloers zijn. De eerste die in contact komen met dergelijke misdrijven is vaak de lokale politie, die dan ook een zekere vorming dient te krijgen. In Nederland investeren ze fenomenale bedragen in de vorming van de lokale recherche, d.m.v. online cursussen e.d., uitbesteed aan private firma‟s. Bij ons geschiedt dat allemaal in eigen huis, wat niet houdbaar is. Nederland is dan ook koploper, niet alleen wat betreft vorming, maar ook qua opzetten van infrastructuur. Daarenboven is men daar ook creatief bezig met de bestrijding van cybercriminaliteit. Dit vooral wat betreft het afbreken van structuren die cybercriminelen gebruiken, of op z‟n minst voorkomen dat het überhaupt wordt opgebouwd. De Nederlanders hebben daar dan ook een onderzoek naar opgezet, net als Luxemburg en het Verenigd Koninkrijk. België is in dat kader eerder de slechte leerling van de

klas. Er is hier dan ook geen overlegstructuur of leidende overheid die de zaken gaat coördineren. Als je dan proactief moet werken moet dit gecontroleerd gebeuren, maar er is geen overheid die daar wat sturing aan geeft. Dat hebben we dan ook broodnodig. Wat de bestrijding van *cybercrime* betreft denk ik dat Nederland erg goed bezig is, al dienen we daar ook kanttekeningen bij te plaatsen. Men heeft daar een solide strategie opgebouwd. Men heeft trouwens in het forensisch laboratorium in Nederland een team voor digitale expertise, waar men de moeilijk gevallen van data recuperatie e.d. gaat uitvoeren. Dat is iets dat wij in België niet hebben. Hier hebben we het CERT, voor de melding van problemen waarvoor de gebruiker niet direct naar de politie wil stappen. In Nederland is een soortgelijke instelling geïntegreerd in het Nationale Cybersecurity Centre, en die instelling was 90 man groot, een enorm aantal. Ter vergelijking, het CERT is 7 man sterk. In Nederland heeft men duidelijk de keuze gemaakt om van *cybercrime* een prioriteit te maken, i.t.t België, waar we alles gaan willen doen, en de capaciteit dan ook als dusdanig wordt gespreid. Het probleem daarvan is dat wanneer je alles wil aanpakken, je weinig echt grondig kan doen. Je verliest als het ware capaciteit om de echt belangrijke zaken aan te pakken. In Nederland snijden ze in het aantal dossiers, maar degene die ze dan afwerken zijn ook tot op het bot uitgespit. Wat er verder ook dient te gebeuren is dat er op federaal niveau, binnen de regering, iemand moet komen die de leiding neemt inzake cyberbeveiliging. In de Verenigde Staten hebben ze dit al. Daar is Howard Schmidt de Cyber-Security Coördinator, die deel uitmaakt van het kabinet van de president zelf. Als je bijvoorbeeld kijkt naar Engeland, daar hebben ze tijdens de crisis Bijlagen 199 op zowat alles bespaard, behalve op de strijd tegen cybercriminaliteit. Integendeel, men heeft destijds ongeveer 600 miljoen pond vrijgemaakt voor de bestrijding van *cybercrime*. Men heeft destijds zelfs oorlogsfregatten verkocht, en de opbrengst ervan in de aanpak van *cybercrime* gepompt. Als je naar die investeringen kijkt, dan kan je besluiten dat we hier niet echt goed bezig zijn. Dit is echter het gevolg van het feit dat de overheid hier zich te weinig bewust lijkt te zijn van de dreiging, en de schade die *cybercrime* teweegbrengt. Als je dan weer vergelijkt met een land als Ierland, dan zijn we nog niet zo slecht bezig. Daar hebben ze 12 mensen die zich met *cybercrime* bezighouden. Wij doen het al bij al niet zo slecht, ook omwille van het feit dat wij één politiedienst hebben. Bij andere landen is dit verspreid over verschillende politiediensten, wat het werk er ook niet makkelijker op maakt. Bij de politiehervorming was het mijn taak om het FCCU op een structurele manier uit te bouwen. Dit zowel wat betreft de rekrutering van het personeel, als de opleiding, maar ook wat betreft materiaal. Dat laatste was de jaren volgend op de politiehervorming de hoofdbrok van mijn inspanningen. In die zin dat ik elk lid wou uitrusten met een forensische toren, een portable en voldoende back-up stations.

Annexe 3. Statistiques du ministère public en matière de criminalité informatique spécifique - Tableau des affaires pendantes au 1/1/2014 selon le type de prévention

Disponible sur : http://www.om-mp.be/stat

	ANVERS		BRUXELLES		GAND		LIEGE		MONS		BELGIQUE	
	n	%	n	%	n	%	n	%	n	%	n	%
(1) CODE PÉNAL	25.915	70,47	38.161	76,05	31.491	74,81	32.905	75,93	41.034	82,64	169.506	76,34
(2) PROPRIETE	11.815	32,13	15.188	30,27	14.830	35,23	11.365	26,23	17.761	35,77	70.959	31,96
(3) vol & extorsion	7.666	20,85	8.475	16,89	9.617	22,84	6.312	14,57	10.026	20,19	42.096	18,96
(4) vol simple	2.789	7,58	3.456	6,89	4.409	10,47	2.170	5,01	4.011	8,08	16.835	7,58
(5) vol avec violence	1.035	2,81	2.381	4,75	756	1,80	1.383	3,19	1.782	3,59	7.337	3,30
(6) vol aggravé	3.842	10,45	2.638	5,26	4.452	10,58	2.759	6,37	4.233	8,52	17.924	8,07
(7) destruction, dégradation & incendie	802	2,18	1.008	2,01	1.530	3,63	1.607	3,71	2.218	4,47	7.165	3,23
(8) fraude	3.347	9,10	5.705	11,37	3.683	8,75	3.446	7,95	5.517	11,11	21.698	9,77
(9) recel & blanchiment	557	1,51	927	1,85	387	0,92	455	1,05	640	1,29	2.966	1,34
(10) informatique	668	1,82	1.178	2,35	750	1,78	639	1,47	1.920	3,87	5.155	2,32
(11) autres	2.122	5,77	3.600	7,17	2.546	6,05	2.352	5,43	2.957	5,96	13.577	6,11
(12) PERSONNE	5.651	15,37	9.632	19,20	7.218	17,15	8.933	20,61	9.437	19,01	40.871	18,41
(13) assassinat, meurtre & homicide involontaire	225	0,61	330	0,66	167	0,40	264	0,61	203	0,41	1.189	0,54
(14) assassinat & meurtre	220	0,60	293	0,58	153	0,36	229	0,53	183	0,37	1.078	0,49
(15) homicide involontaire	5	0,01	37	0,07	14	0,03	35	0,08	20	0,04	111	0,05
(16) coups & blessures	3.592	9,77	6.289	12,53	4.760	11,31	6.044	13,95	6.344	12,78	27.029	12,17
(17) volontaires	3.499	9,52	6.063	12,08	4.597	10,92	5.828	13,45	6.162	12,41	26.149	11,78
(18) involontaires	93	0,25	226	0,45	163	0,39	216	0,50	182	0,37	880	0,40
(19) libertés individuelles	1.834	4,99	3.013	6,00	2.291	5,44	2.625	6,06	2.890	5,82	12.653	5,70
(20) FAMILLE & MORALITE PUBLIQUE	3.533	9,61	2.317	4,62	2.843	6,75	5.088	11,74	4.593	9,25	18.374	8,28

(21)	**viol & attentat à la pudeur**	799	2,17	1.200	2,39	1.120	2,66	1.426	3,29	1.043	2,10	5.588	2,52
(22)	**débauche & exploitation sexuelle**	417	1,13	492	0,98	516	1,23	414	0,96	298	0,60	2.137	0,96
(23)	**sphère familiale**	2.317	6,30	625	1,25	1.207	2,87	3.248	7,49	3.252	6,55	10.649	4,80
(24)	**ORDRE PUBLIC & SECURITE PUBLIQUE**	3.781	10,28	8.438	16,82	5.286	12,56	6.380	14,72	7.749	15,61	31.634	14,25
(25)	**FOI PUBLIQUE**	1.135	3,09	2.586	5,15	1.314	3,12	1.139	2,63	1.494	3,01	7.668	3,45
(26)	**LOIS SPECIALES**	9.766	26,56	10.820	21,56	9.533	22,65	8.797	20,30	6.766	13,63	45.682	20,57
(27)	**SANTE PUBLIQUE**	713	1,94	418	0,83	391	0,93	624	1,44	271	0,55	2.417	1,09
(28)	**STUPEFIANTS & DOPAGE**	3.301	8,98	2.774	5,53	3.046	7,24	1.925	4,44	1.594	3,21	12.640	5,69
(29)	**AFFAIRES ECONOMIQUES**	489	1,33	1.151	2,29	359	0,85	425	0,98	493	0,99	2.917	1,31
(30)	**ENVIRONNEMENT & URBANISME**	2.319	6,31	2.179	4,34	2.316	5,50	1.626	3,75	874	1,76	9.314	4,19
(31)	**environnement**	892	2,43	635	1,27	854	2,03	739	1,71	569	1,15	3.689	1,66
(32)	**urbanisme**	1.427	3,88	1.544	3,08	1.462	3,47	887	2,05	305	0,61	5.625	2,53
(33)	**AGRICULTURE, CHASSE, PECHE & PROTECTION DES ANIMAUX**	300	0,82	170	0,34	317	0,75	576	1,33	181	0,36	1.544	0,70
(34)	**TRAVAIL & SECURITE SOCIALE**	52	0,14	82	0,16	82	0,19	69	0,16	124	0,25	409	0,18
(35)	**AFFAIRES FINANCIERES**	2.592	7,05	4.046	8,06	3.022	7,18	3.552	8,20	3.229	6,50	16.441	7,40
(36)	**général**	2.483	6,75	3.877	7,73	2.789	6,63	3.342	7,71	3.052	6,15	15.543	7,00
(37)	**fraude fiscale**	109	0,30	169	0,34	233	0,55	210	0,48	177	0,36	898	0,40
(38)	**MATIERE PARQUETS DE POLICE**	54	0,15	157	0,31	6	0,01	171	0,39	57	0,11	445	0,20
(39)	**AUTRE**	1.038	2,82	1.039	2,07	1.067	2,53	1.463	3,38	1.797	3,62	6.404	2,88

Annexe 4. Statistiques du ministère public en matière de criminalité informatique spécifique - Flux d'entrée des affaires au cours de 2014 par ressort judiciaire selon le type de prévention (N et %)

Disponible sur : http://www.om-mp.be/stat

	ANVERS		BRUXELLES		GAND		LIEGE		MONS		BELGIQUE	
	n	%	n	%	n	%	n	%	n	%	n	%
(1) CODE PENAL	98.756	77,36	122.874	77,97	118.655	79,05	116.201	81,83	87.246	83,39	543.732	79,73
(2) PROPRIETE	51.245	40,14	67.049	42,54	60.354	40,21	58.170	40,96	47.006	44,93	283.824	41,62
(3) vol & extorsion	35.101	27,50	46.129	29,27	39.996	26,64	38.000	26,76	30.093	28,76	189.319	27,76
(4) vol simple	14.367	11,25	18.997	12,05	17.887	11,92	11.939	8,41	11.215	10,72	74.405	10,91
(5) vol avec violence	3.375	2,64	8.076	5,12	2.388	1,59	3.788	2,67	3.599	3,44	21.226	3,11
(6) vol aggravé	17.359	13,60	19.056	12,09	19.721	13,14	22.273	15,68	15.279	14,60	93.688	13,74
(7) destruction, dégradation & incendie	4.238	3,32	4.327	2,75	5.952	3,97	7.590	5,34	5.780	5,52	27.887	4,09
(8) fraude	11.906	9,33	16.593	10,53	14.406	9,60	12.580	8,86	11.133	10,64	66.618	9,77
(9) recel & blanchiment	732	0,57	1.754	1,11	601	0,40	835	0,59	697	0,67	4.619	0,68
(10) informatique	2.678	2,10	5.277	3,35	3.168	2,11	3.228	2,27	4.541	4,34	18.892	2,77
(11) autres	8.496	6,66	9.562	6,07	10.637	7,09	8.517	6,00	5.895	5,63	43.107	6,32
(12) PERSONNE	21.744	17,03	23.889	15,16	24.541	16,35	23.422	16,49	17.218	16,46	110.814	16,25
(13) assassinat, meurtre & homicide involontaire	274	0,21	364	0,23	222	0,15	238	0,17	192	0,18	1.290	0,19
(14) assassinat & meurtre	265	0,21	351	0,22	214	0,14	225	0,16	178	0,17	1.233	0,18
(15) homicide involontaire	9	0,01	13	0,01	8	0,01	13	0,01	14	0,01	57	0,01
(16) coups & blessures	13.775	10,79	15.229	9,66	14.362	9,57	14.764	10,40	11.246	10,75	69.376	10,17
(17) volontaires	13.311	10,43	14.523	9,22	13.492	8,99	14.005	9,86	10.882	10,40	66.213	9,71
(18) involontaires	464	0,36	706	0,45	870	0,58	759	0,53	364	0,35	3.163	0,46
(19) libertés individuelles	7.695	6,03	8.296	5,26	9.957	6,63	8.420	5,93	5.780	5,52	40.148	5,89
(20) FAMILLE & MORALITE PUBLIQUE	8.339	6,53	7.456	4,73	10.382	6,92	10.456	7,36	6.674	6,38	43.307	6,35
(21) viol & attentat à la pudeur	1.797	1,41	1.807	1,15	1.787	1,19	1.435	1,01	1.060	1,01	7.886	1,16

	ANVERS		BRUXELLES		GAND		LIEGE		MONS		BELGIQUE	
	n	%	n	%	n	%	n	%	n	%	n	%
(22) débauche & exploitation sexuelle	881	0,69	1.338	0,85	1.027	0,68	646	0,45	399	0,38	4.291	0,63
(23) sphère familiale	5.661	4,43	4.311	2,74	7.568	5,04	8.375	5,90	5.215	4,98	31.130	4,56
(24) ORDRE PUBLIC & SECURITE PUBLIQUE	14.665	11,49	19.132	12,14	20.345	13,55	21.376	15,05	14.315	13,68	89.833	13,17
(25) FOI PUBLIQUE	2.763	2,16	5.348	3,39	3.033	2,02	2.777	1,96	2.033	1,94	15.954	2,34
(26) LOIS SPECIALES	23.969	18,78	29.584	18,77	23.938	15,95	18.552	13,06	12.587	12,03	108.630	15,93
(27) SANTE PUBLIQUE	2.462	1,93	3.211	2,04	2.114	1,41	1.452	1,02	1.594	1,52	10.833	1,59
(28) STUPEFIANTS & DOPAGE	11.675	9,15	7.551	4,79	8.757	5,83	5.673	3,99	3.602	3,44	37.258	5,46
(29) AFFAIRES ECONOMIQUES	1.090	0,85	2.445	1,55	1.891	1,26	989	0,70	649	0,62	7.064	1,04
(30) ENVIRONNEMENT & URBANISME	2.674	2,09	7.378	4,68	3.665	2,44	5.232	3,68	3.255	3,11	22.204	3,26
(31) environnement	1.353	1,06	5.862	3,72	2.305	1,54	4.009	2,82	2.197	2,10	15.726	2,31
(32) urbanisme	1.321	1,03	1.516	0,96	1.360	0,91	1.223	0,86	1.058	1,01	6.478	0,95
(33) AGRICULTURE, CHASSE, PECHE & PROTECTION DES ANIMAUX	798	0,63	585	0,37	1.095	0,73	1.092	0,77	438	0,42	4.008	0,59
(34) TRAVAIL & SECURITE SOCIALE	214	0,17	314	0,20	334	0,22	322	0,23	254	0,24	1.438	0,21
(35) AFFAIRES FINANCIERES	5.056	3,96	8.100	5,14	6.082	4,05	3.792	2,67	2.795	2,67	25.825	3,79
(36) général	4.944	3,87	7.846	4,98	5.784	3,85	3.542	2,49	2.703	2,58	24.819	3,64
(37) fraude fiscale	112	0,09	254	0,16	298	0,20	250	0,18	92	0,09	1.006	0,15
(38) MATIERE PARQUETS DE POLICE	224	0,18	27	0,02	49	0,03	47	0,03	18	0,02	365	0,05
(39) AUTRE	4.712	3,69	5.113	3,24	7.467	4,97	7.203	5,07	4.773	4,56	29.268	4,29
TOTAL	127.661	100,00	157.598	100,00	150.109	100,00	142.003	100,00	104.624	100,00	681.995	100,00
inconnu/erreur	0	-	0	-	0	-	1	-	0	-	1	-

Annexe 5. Statistiques du ministère public en matière de criminalité informatique spécifique - Flux de sortie des affaires au cours de 2014 par ressort judiciaire : décisions de clôture selon le type de prévention (N et %)

Disponible sur : http://www.om-mp.be/stat

BELGIQUE

	sans suite		pour disposition		jonction		transaction payée		médiation pénale finie		citation directe		chambre du conseil		TOTAL	
	n	%	n	%	n	%	n	%	n	%	n	%	n	%	n	%
(1) CODE PÉNAL	388.121	80,18	44.067	76,78	67.164	82,75	4.166	56,58	2.460	89,03	15.556	79,25	11.136	75,87	532.670	79,86
(2) PROPRIETE	211.075	43,61	22.885	39,87	34.283	42,24	954	12,96	713	25,81	6.223	31,70	5.118	34,87	281.251	42,16
(3) vol & extorsion	145.776	30,12	12.613	21,98	20.969	25,84	823	11,18	481	17,41	4.949	25,21	3.748	25,54	189.359	28,39
(4) vol simple	51.520	10,64	6.998	12,19	10.231	12,61	789	10,72	362	13,10	2.989	15,23	839	5,72	73.728	11,05
(5) vol avec violence	16.117	3,33	1.440	2,51	1.537	1,89	11	0,15	33	1,19	727	3,70	1.393	9,49	21.258	3,19
(6) vol aggravé	78.139	16,14	4.175	7,27	9.201	11,34	23	0,31	86	3,11	1.233	6,28	1.516	10,33	94.373	14,15
(7) destruction, dégradation & incendie	22.716	4,69	1.154	2,01	3.008	3,71	28	0,38	121	4,38	354	1,80	241	1,64	27.622	4,14
(8) fraude	42.583	8,80	9.118	15,89	10.306	12,70	103	1,40	111	4,02	920	4,69	1.129	7,69	64.270	9,64
(9) recel & blanchiment	2.486	0,51	543	0,95	1.005	1,24	33	0,45	4	0,14	131	0,67	130	0,89	4.332	0,65
(10) informatique	12.000	2,48	1.728	3,01	3.992	4,92	6	0,08	47	1,70	132	0,67	124	0,84	18.029	2,70
(11) autres	28.097	5,80	6.847	11,93	5.309	6,54	64	0,87	60	2,17	657	3,35	875	5,96	41.909	6,28
(12) PERSONNE	79.176	16,36	6.695	11,66	12.518	15,42	134	1,82	1.266	45,82	4.118	20,98	3.162	21,54	107.069	16,05
(13) assassinat, meurtre & homicide involontaire	250	0,05	62	0,11	256	0,32	0	0,00	5	0,18	49	0,25	652	4,44	1.274	0,19
(14) assassinat & meurtre	231	0,05	59	0,10	248	0,31	0	0,00	5	0,18	48	0,24	615	4,19	1.206	0,18
(15) homicide involontaire	19	0,00	3	0,01	8	0,01	0	0,00	0	0,00	1	0,01	37	0,25	68	0,01
(16) coups & blessures	49.770	10,28	3.629	6,32	6.868	8,46	72	0,98	1.188	43,00	3.786	19,29	1.767	12,04	67.080	10,06
(17) volontaires	47.279	9,77	3.207	5,59	6.758	8,33	69	0,94	1.175	42,53	3.756	19,13	1.703	11,60	63.947	9,59
(18) involontaires	2.491	0,51	422	0,74	110	0,14	3	0,04	13	0,47	30	0,15	64	0,44	3.133	0,47
(19) libertés individuelles	29.156	6,02	3.004	5,23	5.394	6,65	62	0,84	73	2,64	283	1,44	743	5,06	38.715	5,80

BELGIQUE

	sans suite		pour disposition		jonction		transaction payée		médiation pénale finie		citation directe		chambre du conseil		TOTAL	
	n	%	n	%	n	%	n	%	n	%	n	%	n	%	n	%
(20) FAMILLE & MORALITE PUBLIQUE	25.139	5,19	5.850	10,19	8.269	10,19	28	0,38	216	7,82	862	4,39	1.093	7,45	41.457	6,22
(21) viol & attentat à la pudeur	4.550	0,94	973	1,70	1.082	1,33	1	0,01	51	1,85	351	1,79	765	5,21	7.773	1,17
(22) débauche & exploitation sexuelle	2.654	0,55	404	0,70	602	0,74	21	0,29	60	2,17	174	0,89	208	1,42	4.123	0,62
(23) sphère familiale	17.935	3,71	4.473	7,79	6.585	8,11	6	0,08	105	3,80	337	1,72	120	0,82	29.561	4,43
(24) ORDRE PUBLIC & SECURITE PUBLIQUE	62.521	12,92	6.491	11,31	10.022	12,35	2.886	39,20	216	7,82	3.878	19,76	1.123	7,65	87.137	13,06
(25) FOI PUBLIQUE	10.210	2,11	2.146	3,74	2.072	2,55	164	2,23	49	1,77	475	2,42	640	4,36	15.756	2,36
(26) LOIS SPECIALES	72.366	14,95	10.103	17,60	12.327	15,19	3.191	43,34	291	10,53	3.977	20,26	3.085	21,02	105.340	15,79
(27) SANTE PUBLIQUE	8.348	1,72	547	0,95	897	1,11	265	3,60	5	0,18	402	2,05	42	0,29	10.506	1,58
(28) STUPEFIANTS & DOPAGE	19.546	4,04	4.301	7,49	3.673	4,53	2.410	32,73	282	10,21	2.199	11,20	2.674	18,22	35.085	5,26
(29) AFFAIRES ECONOMIQUES	5.866	1,21	379	0,66	906	1,12	142	1,93	0	0,00	172	0,88	36	0,25	7.501	1,12
(30) ENVIRONNEMENT & URBANISME	19.218	3,97	527	0,92	1.303	1,61	296	4,02	3	0,11	506	2,58	19	0,13	21.872	3,28
(31) environnement	13.667	2,82	405	0,71	661	0,81	259	3,52	3	0,11	300	1,53	9	0,06	15.304	2,29
(32) urbanisme	5.551	1,15	122	0,21	642	0,79	37	0,50	0	0,00	206	1,05	10	0,07	6.568	0,98
(33) AGRICULTURE, CHASSE, PECHE & PROTECTION DES ANIMAUX	2.878	0,59	259	0,45	292	0,36	66	0,90	1	0,04	168	0,86	16	0,11	3.680	0,55
(34) TRAVAIL & SECURITE SOCIALE	483	0,10	806	1,40	91	0,11	4	0,05	0	0,00	66	0,34	2	0,01	1.452	0,22
(35) AFFAIRES FINANCIERES	16.027	3,31	3.284	5,72	5.165	6,36	8	0,11	0	0,00	464	2,36	296	2,02	25.244	3,78
(36) général	15.515	3,21	3.112	5,42	5.063	6,24	5	0,07	0	0,00	355	1,81	261	1,78	24.311	3,64
(37) fraude fiscale	512	0,11	172	0,30	102	0,13	3	0,04	0	0,00	109	0,56	35	0,24	933	0,14
(38) MATIERE PARQUETS DE POLICE	164	0,03	39	0,07	36	0,04	0	0,00	0	0,00	39	0,20	34	0,23	312	0,05
(39) AUTRE	23.395	4,83	3.188	5,55	1.635	2,01	6	0,08	12	0,43	58	0,30	422	2,88	28.716	4,31
TOTAL	484.046	100,00	57.397	100,00	81.162	100,00	7.363	100,00	2.763	100,00	19.630	100,00	14.677	100,00	667.038	100,00
inconnu/erreur	0	-	0	-	1	-	0	-	0	-	0	-	0	-	1	-

Annexe 6. Statistiques à propos de la disponibilité de l'Internet dans le ménage en Belgique

Pourcentage de ménages belges comptant au moins une personne âgée entre 16 et 74 ans

Disponible sur : http://StatBel.fgov.be/

2014	Total	Ménages sans enfants				Ménages avec enfants				Densité de population du lieu de résidence		
		Total	1 adulte	2 ad.	> 2 ad.	Total	1 adulte	2 ad.	> 2 ad.	Faible	Interméd.	Haute
Ménage disposant d'une connexion Internet	83%	78%	67%	82%	95%	94%	89%	95%	95%	77%	85%	82%
Ménage ne disposant plus de connexion Internet	2%	2%	4%	1%	1%	1%	2%	1%	2%	3%	2%	2%
Ménage n'ayant jamais eu de connexion Internet	15%	19%	28%	16%	5%	4%	9%	4%	3%	19%	13%	16%
Ménage ne disposant pas de connexion Internet	17%	22%	33%	18%	5%	6%	11%	5%	5%	23%	15%	18%

Annexe 7. Statistiques EuroStat sur l'accès à Internet dans les ménages à niveau européen

Disponible sur le site web d'EuroStats: http://www.ec.europa.eu/eurostat/statistics-explained

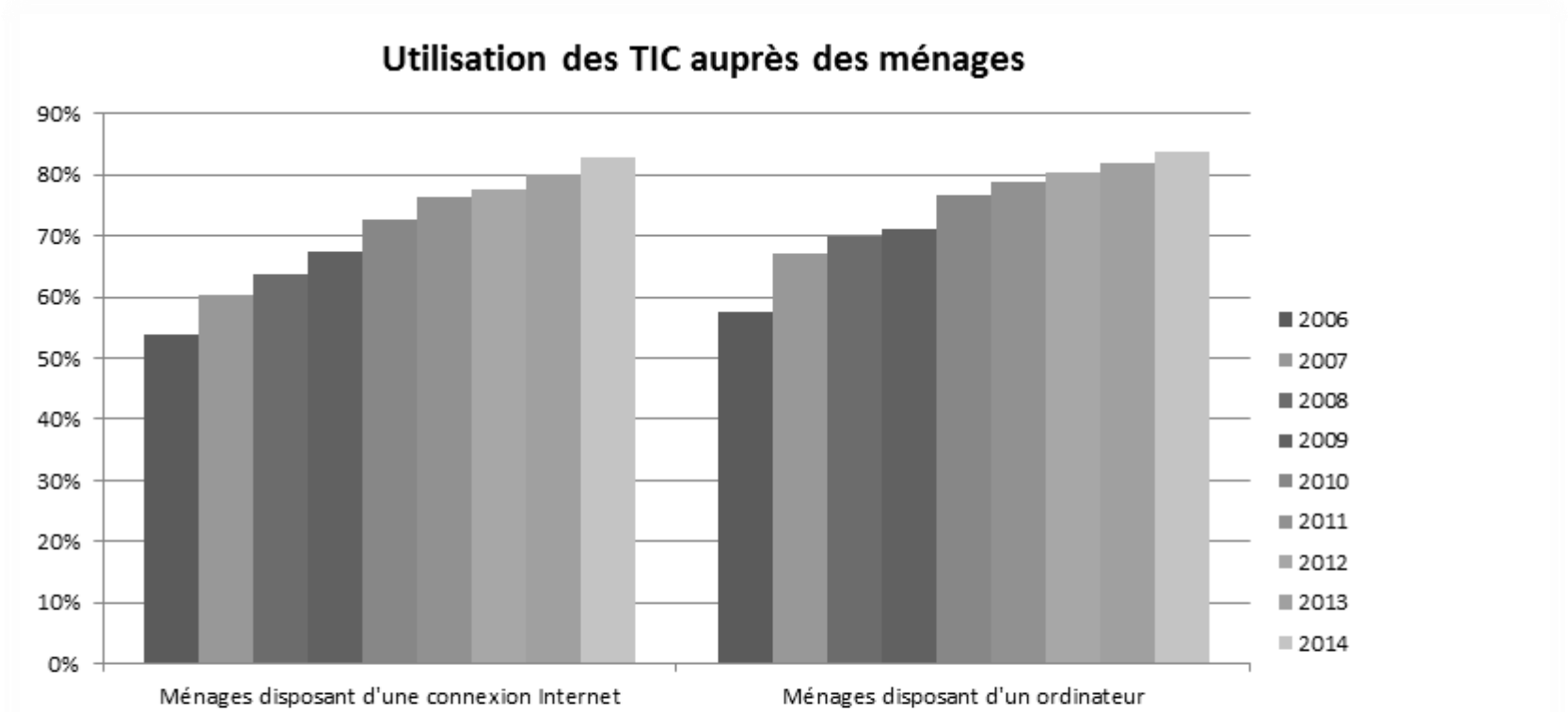
Level of Internet access - households												
geo\time	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014
EU (28 countries)	:	:	:	:	55	60	66	70	73	76	79	81
EU (27 countries)	:	41	48	49	55	60	66	70	73	76	79	81
Euro area (changing composition)	40	44	50	51	57	62	67	71	74	76	79	81
Euro area (18 countries)	:	:	:	:	:	:	:	:	:	:	:	:
Euro area (17 countries)	:	:	:	:	:	:	:	:	:	:	:	:
Belgium	:	:	50	54	60	64	67	73	77	78	80	83
Bulgaria	:	10	:	17	19	25	30	33	45	51	54	57
Czech Republic	15	19	19	29	35	46	54	61	67	65	73	78
Denmark	64	69	75	79	78	82	83	86	90	92	93	93
Germany	54	60	62	67	71	75	79	82	83	85	88	89
Estonia	:	31	37	45	52	57	62	67	69	74	79	83
Ireland	36	40	47	50	57	63	67	72	78	81	82	82
Greece	16	17	22	23	25	31	38	46	50	54	56	66
Spain	28	34	36	38	43	50	53	58	63	67	70	74
France	31	34	:	41	55	62	69	74	76	80	82	83
Croatia	:	:	:	:	41	45	50	56	61	66	65	68
Italy	32	34	39	40	43	47	53	59	62	63	69	73
Cyprus	29	53	32	37	39	43	53	54	57	62	65	69

geo\time	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014
Latvia	:	15	31	42	51	53	58	60	64	69	72	73
Lithuania	6	12	16	35	44	51	60	61	60	60	65	66
Luxembourg	45	59	65	70	75	80	87	90	91	93	94	96
Hungary	:	14	22	32	38	48	55	60	65	69	71	75
Malta	:	:	41	53	54	59	64	70	75	77	79	81
Netherlands	61	65	78	80	83	86	90	91	94	94	95	96
Austria	37	45	47	52	60	69	70	73	75	79	81	81
Poland	14	26	30	36	41	48	59	63	67	70	72	75
Portugal	22	26	31	35	40	46	48	54	58	61	62	65
Romania	:	6	:	14	22	30	38	42	47	54	58	61
Slovenia	:	47	48	54	58	59	64	68	73	74	76	77
Slovakia	:	23	23	27	46	58	62	67	71	75	78	78
Finland	47	51	54	65	69	72	78	81	84	87	89	90
Sweden	:	:	73	77	79	84	86	88	91	92	93	90
United Kingdom	55	56	60	63	67	71	77	80	83	87	88	90
Iceland	:	81	84	83	84	88	90	92	93	95	96	96
Liechtenstein	:	:	:	:	:	:	:	:	:	:	:	:
Norway	60	60	64	69	78	84	86	90	92	93	94	93
Switzerland	:	:	:	:	:	:	:	:	:	:	:	91
Montenegro	:	:	:	:	:	:	:	:	:	55	:	:
Former Yugoslav Republic of Macedonia, the	:	11	:	14	:	29	42	46	:	58	65	68
Serbia	:	:	:	:	26	:	37	:	:	:	:	:
Turkey	:	7	8	:	20	25	30	42	:	47	49	60
Canada	55	60	61	:	:	:	:	:	:	:	:	:
United States	55	:	:	:	:	:	:	:	:	:	:	:
Japan	54	56	57	:	:	:	:	:	:	:	:	:
South Korea	69	86	92	:	:	:	:	:	:	:	:	:
Australia	53	56	:	:	:	:	:	:	:	:	:	:

Annexe 8. Statistiques à propos de l'utilisation des TIC auprès des ménages

Ménages disposant d'une connexion internet et ménages disposant d'un ordinateur

Disponible sur : http://StatBel.fgov.be/



Annexe 9. Flux d'entrée des affaires de type « informatique » de 2003 à 2014

Tableau établi par Caroline Heymans sur base des statistiques du ministère public, disponibles sur : http://www.om-mp.be/stat

	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014
Informatique	1 034	1 771	3 276	4 732	7 831	9 867	12 631	17 346	16 217	2 1492[322]	19 847	18 892

[322] Le pic de 2012 s'explique par une croissante utilisation de *police ransomware* à cet époque qui dura en 2012 et début 2013. En laissant ce pic de coté, nous pouvons observer une croissance continue sur les dix dernières années.

Angry Birds 2, nouvel opus du célèbre jeu, lancé seulement jeudi dernier, s'est déjà emparé de la première place des téléchargements gratuits sur iPhone et iPad en France. © Dr.

ÉCONOMIE

L'accès à nos données sera mieux encadré

TÉLÉCOMS Le gouvernement corrige le tir après l'annulation de la loi

- La loi sur la conservation des communications électroniques violait le droit au respect de la vie privée.
- Un nouvel avant-projet de loi est prêt.
- Toutes les données ne devront plus être conservées douze mois.

Un mois et demi seulement après l'annulation par la Cour constitutionnelle de la loi sur la conservation des données, un nouvel avant-projet de loi répondant à ses critiques est déjà prêt. Pas question pour le gouvernement de laisser trop longtemps la justice dans le flou et de pénaliser des enquêtes. Rédigé par les trois ministres compétents, Alexander De Croo (Télécoms), Koen Geens (Justice) et Steven Vandeput (Défense), il est actuellement soumis à la consultation publique par l'IBPT, le régulateur des télécoms.

Cette loi polémique organise la conservation par les opérateurs des communications électroniques. Votée en 2013, elle imposait aux fournisseurs d'accès de stocker durant un an toutes les données relatives aux appels téléphoniques, les sessions de connexion à internet, les adresses d'origine et de destination des courriers électroniques, les adresses des sites visités ainsi que les dates de ces visites. Le contenu des mails ou des communications téléphoniques n'était pas concerné.

En juin, le texte a été annulé par la Cour constitutionnelle après un recours introduit par La Ligue des droits de l'homme et l'Ordre des barreaux d'avocats francophones et germanophone. Motif invoqué ? Une limitation disproportionnée du droit au respect de la vie privée. Rien d'étonnant en soi puisque la directive européenne dont elle n'était qu'une transposition avait elle-même été invalidée par la Cour européenne de justice. Quatre reproches étaient adressés au législateur belge par la Cour. Voici les réponses apportées.

1 Pas de distinction entre les personnes. La Cour déplore la conservation des données de façon indifférenciée, sans distinction entre les personnes, les zones géographiques, la période. Le gouvernement estime ne pas pouvoir changer de cap sur ce point. *« Limiter la conservation des données à celles concernant des personnes qui font déjà l'objet d'une enquête pénale ou de renseignement n'a pas de sens car cette possibilité existe déjà par ailleurs. Les autorités judiciaires comme les services de renseignement peuvent déjà imposer le repérage des communications dans le cadre d'une enquête précise »*, peut-on lire. L'objectif de la loi est précisément de pouvoir retrouver des informations dans le passé sur des personnes qui ne font pas encore nécessairement l'objet d'une enquête. Cibler préalablement des personnes en fonction de certains critères reviendrait à encourager une sorte de délit de faciès électronique.

2 Pas de distinction entre les catégories de données. En matière de durée de conservation des données, la Cour reprochait à la loi l'absence de distinction entre les différentes catégories de données. Le nouveau texte comble cette lacune. Quatre catégories sont constituées. Les données d'identification (qui se cachent derrière tel numéro ou telle adresse) seront conservées 12 mois. Les données de communication (quel volume de données consommé, quel type d'abonnement...) ? Deux mois. Pour les deux autres catégories : les données de connexion et de localisation (le lieu et la durée de la communication) et les données personnelles (qui a appelé ou écrit à qui ?), le législateur n'a toujours pas tranché sur la durée de conservation. Ce sera neuf ou douze mois.

3 Absence d'encadrement pour l'accès aux données conservées. Le gouvernement répond à cette critique en renforçant les conditions d'accès fixées dans le Code d'instruction criminelle et dans la loi sur les services de renseignement. L'accès pour la justice ne sera autorisé que si le résultat ne peut pas être atteint par une autre mesure moins intrusive. Une différenciation sera faite sur base de la gravité de l'infraction. Pour les infractions punies d'une peine de moins d'un an d'emprisonnement, l'accès à ces données sera interdit. De un à cinq ans d'emprisonnement, l'accès sera limité aux données relatives aux six derniers mois. Pour les infractions de plus de cinq ans ou commises dans le cadre d'une organisation criminelle, la mesure pourra porter sur l'entièreté de la durée de conservation.

Une protection spéciale sera accordée aux médecins, aux avocats (secret professionnel) et aux journalistes (secret des sources). Il sera interdit aux services de renseignement d'obtenir des données protégées par ces secrets à moins qu'ils ne disposent au préalable d'indices sérieux selon lesquels l'avocat, le médecin ou le journaliste prend activement part à une menace. Dans ce cas, les services de renseignement devront au préalable en informer l'organisation professionnelle de la personne.

La nouvelle loi permet à trois autres « institutions » d'accéder aux communications conservées : les services d'urgence, le service médiation (pour identifier les auteurs d'appels malveillants) et la cellule personnes disparues.

4 Une sécurisation des données insuffisante. Des obligations en termes de cryptage et de destruction des données à l'expiration du délai sont prévues. Chaque entreprise devra désigner un préposé à la protection des données chargé de veiller au respect des règles. ■

JEAN-FRANÇOIS MUNSTER

RÉACTION

« On réattaquera cette loi »

Jean-François Henrotte est, avec Eric Lemmens, l'avocat de l'Ordre des barreaux des avocats francophones et germanophone qui avait introduit le recours contre la première mouture de la loi. Même s'il reconnaît qu'il y a des progrès dans le nouveau texte, il subsiste pour lui des problèmes fondamentaux. *« Sur l'argument principal de la Cour, à savoir le fait que la conservation des données ne peut concerner tout le monde sans distinction, le gouvernement rétorque que la Cour se trompe, qu'il ne sait pas rencontrer ses demandes et qu'il passe donc outre. Cela laisse rêveur d'un point de vue juridique. Il signe lui-même le recours que l'on introduira. »* Il regrette en particulier que le législateur continue de dire qu'il n'est pas possible d'exclure les avocats du système de récolte des données puisqu'il est impossible de les identifier comme tels. *« Faux,* rétorque Jean-François Henrotte. *Nous avons des lignes Internet fixes dédiées. Ce n'est pas compliqué de savoir qu'un avocat se trouve derrière l'une d'elles. »*

J.-F. M.

© PHOTO NEWS.

« *La révolution informatique a fourni les outils permettant de voler en toute impunité, de contrôler et de manipuler les pensées et les mouvements de millions de gens et de tenir une société entière en otage. D'un autre coté s'il est bien employé, l'ordinateur peut améliorer de façon notable la vie de milliards d'habitants de la planète. Le choix est dans nos mains. L'avenir de l'humanité ne doit pas obligatoirement être un avenir de criminalité informatique et de terreur* »

- August BEQUAI
Washington DC, avril 1990

À l'heure où l'accès aux nouvelles technologies est quasi-généralisé en Belgique et que la cybercriminalité ne cesse d'augmenter, il convient de se demander dans quelle mesure notre droit pénal matériel et procédural est efficace pour lutter contre ce phénomène grandissant.

Le présent mémoire constitue une analyse critique du droit pénal matériel et procédural en la matière en pointant du doigt les problèmes qui subsistent à l'heure d'aujourd'hui.

À travers la lecture de ce mémoire, le lecteur prendra conscience de l'importance de la criminalité informatique et de la nécessité de déployer rapidement tous les moyens pour lutter contre celle-ci avant que les cyberdélinquants n'acquièrent une trop grande longueur d'avance.

Place Montesquieu, 2 bte L2.07.01, 1348 Louvain-la-Neuve, Belgique **www.uclouvain.be/drt**