Conseil de
l'Union européenne

Bruxelles, le 18 août 2017
(OR. fr, en)

8212/1/17
REV 1 DCL 1

GENVAL 43
CYBER 58

DÉCLASSIFICATION

du document:	8212/1/17 REV 1 RESTREINT UE/EU RESTRICTED
en date du:	18 mai 2017
Nouveau statut:	Public
Objet:	Rapport d'évaluation sur la septième série d'évaluations mutuelles "Mise en œuvre pratique et fonctionnement des politiques européennes en matière de prévention de la cybercriminalité et de lutte contre celle-ci" - Rapport sur la Belgique

Les délégations trouveront ci-joint la version déclassifiée du document cité en objet.

Le texte de ce document est identique à celui de la version précédente.

Conseil de
l'Union européenne

Bruxelles, le 18 mai 2017
(OR. fr, en)

8212/1/17
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 43
CYBER 58

RAPPORT

Objet:	Rapport d'évaluation sur la septième série d'évaluations mutuelles "Mise en œuvre pratique et fonctionnement des politiques européennes en matière de prévention de la cybercriminalité et de lutte contre celle-ci" - Rapport sur la Belgique

ANNEXE

Table des matières

1 RÉSUMÉ

D'une manière générale, l'équipe d'évaluation estime que les autorités belges sont conscientes des défis liés à la cybercriminalité et qu'elles s'emploient dans plusieurs domaines (juridique, procédural et institutionnel) à renforcer les capacités du pays visant à prévenir et à combattre ce phénomène.
Il convient de signaler que la cybersécurité figure parmi les dix principaux phénomènes sécuritaires abordés dans le plan national de sécurité 2016-2019, qui a été fourni à l'équipe d'évaluation après la visite.

Cependant, le budget consacré à la lutte contre la cybercriminalité est trop restreint en matière de moyens et de formation, de même qu'il existe une pénurie accrue dans les effectifs de police. En particulier, c'est le cas de la FCCU, responsable pour les analyses technico-légales des dossiers des services centraux OCDEFO, OCRC et les services d'inspection, pour les enquêtes en matière d'attaques aux systèmes d'information et aussi pour la formation des unités de police régionales. Ce rôle complexe demande un budget suffisant parce que, de nos jours, l'investigation numérique revêt une importance capitale pour toutes les formes d'activités criminelles, y compris le terrorisme.

L'absence d'intégration des statistiques en matière de cybercriminalité (services de police et système judiciaire - parquets et tribunaux, et les CERT nationaux) est un sujet sur lequel les autorités belges devraient se pencher davantage. Il n'y a pas d'harmonisation des critères relatifs à la collecte des données et aucun lien n'existe entre les données collectées.

En ce qui concerne la législation en matière de cybercriminalité, l'équipe d'évaluation considère que le code pénal belge prévoit toutes les incriminations pertinentes. À l'époque de la visite, le seul changement qui était prévu afin de mettre en œuvre la directive 2013/40 dans son intégralité consistait dans l'alourdissement des sanctions en cas d'accès non autorisé (article 550 *bis*) et d'écoute illicite de communications (article 314 *bis*). Il faut mentionner qu'après la visite d'évaluation un projet de loi[1] a été publie le 16 janvier 2017, qui prévoit des alourdissements de sanctions afin de mettre en œuvre la directive 2013/40.

L'équipe d'évaluation souligne qu'un travail très approfondi et de qualité a été accompli par la FCCU et le Parquet en vue de développer une spécialisation dans l'approche en matière de cybercriminalité.

Dans les services répressifs, les unités chargées de la lutte contre la cybercriminalité ou d'analyse technico-légale des preuves digitales devraient adopter une approche stratégique et unifiée, associant la Police fédérale et les polices locales, afin de coordonner les activités de la FCCU, des RCCU et des LCCU.

Il serait également opportun que les membres de la magistrature, notamment les juges d'instruction, approfondissent leur spécialisation en cybercriminalité.

Cependant, il n'existe pas de règles régissant la coordination entre les services de police au niveau fédéral et au niveau local. Cette lacune est source de dysfonctionnements liés à la multiplicité des unités de police s'occupant de cybercriminalité ou d'analyse technico-légale des preuves digitales – la FCCU, les RCCU et les LCCU – sans aucune vision stratégique. Cela explique l'absence de normes techniques ou procédurales pour les interventions communes, même lorsque les deux unités concernées ont conclu un "gentlemen's agreement".

[1] http://www.dekamer.be/FLWB/PDF/54/2259/54K2259001.pdf

En Belgique, il existe beaucoup d'initiatives publiques et privées concernant les campagnes de prévention de la pédophilie.

Un effort devrait être fait pour sensibiliser davantage le public à la dénonciation des cyberattaques, dans le but d'accroître la capacité de lutter contre la cybercriminalité.

L'institut de formation judiciaire assure une formation de qualité sur la cybercriminalité, destinée aux nouveaux magistrats. Ce modèle pourrait être appliqué aussi aux magistrats ayant une certaine ancienneté.

2 INTRODUCTION

À la suite de l'adoption de l'action commune 97/827/JAI du 5 décembre 1997[2], un mécanisme d'évaluation de l'application et de la mise en œuvre au niveau national des engagements internationaux en matière de lutte contre la criminalité organisée avait été mis en place. Conformément à l'article 2, le groupe "Questions générales, y compris l'évaluation" (GENVAL) a décidé, lors de la réunion du 3 octobre 2013, que la septième série d'évaluations mutuelles serait consacrée à la mise en œuvre pratique et au fonctionnement des politiques européennes en matière de prévention de la cybercriminalité et de lutte contre celle-ci.

Les États membres ont accueilli favorablement le choix de la cybercriminalité comme objet de la septième série d'évaluations mutuelles. Toutefois, compte tenu du large éventail d'infractions qui relèvent de la cybercriminalité, il a été décidé de concentrer l'évaluation sur les infractions auxquelles les États membres estiment qu'il convient d'accorder une attention particulière. À cette fin, l'évaluation porte sur trois domaines spécifiques, à savoir les cyberattaques, les abus sexuels commis en ligne contre des mineurs et la pédopornographie sur l'internet, et la fraude en ligne aux cartes de paiement; elle devrait fournir un examen complet des aspects juridiques et opérationnels de la lutte contre la cybercriminalité, de la coopération transfrontière et de la coopération avec les agences compétentes de l'UE. La directive 2011/93/UE relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants ainsi que la pédopornographie[3] (date de transposition: 18 décembre 2013) et la directive 2013/40/UE relative aux attaques contre les systèmes d'information[4] (date de transposition: 4 septembre 2015) revêtent une importance particulière dans ce contexte.

[2] Action commune 97/827/JAI du 5 décembre 1997, JO L 344 du 15.12.1997, p. 7 à 9.
[3] JO L 335 du 17.12.2011, p. 1.
[4] JO L 218 du 14.8.2013, p. 8.

En outre, dans ses conclusions de juin 2013 concernant la stratégie de cybersécurité de l'UE[5], le Conseil rappelle l'objectif visant à ratifier dans les meilleurs délais la convention du Conseil de l'Europe du 23 novembre 2001 sur la cybercriminalité (convention de Budapest)[6] et souligne dans ses considérants que "l'UE ne préconise pas la création de nouveaux instruments juridiques internationaux concernant les questions inhérentes au cyberespace". La convention de Budapest s'accompagne d'un protocole relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques[7].

L'expérience des évaluations précédentes montre que la mise en œuvre des instruments juridiques concernés est à des stades différents selon les États membres; le processus d'évaluation en cours pourrait aussi apporter une contribution utile aux États membres qui n'auraient pas mis en œuvre tous les aspects des divers instruments. L'évaluation se veut néanmoins large et interdisciplinaire; elle ne se concentre pas uniquement sur la mise en œuvre des différents instruments en matière de lutte contre la cybercriminalité mais aussi sur les aspects opérationnels dans les États membres.

Dès lors, outre la coopération avec les services chargés des poursuites, elle couvrira également la coopération entre les autorités de police, d'une part, et Eurojust, l'ENISA et Europol/EC3, d'autre part, et le retour d'informations de ces acteurs vers les services de police et les services sociaux compétents. L'évaluation se concentre sur la mise en œuvre des politiques nationales en ce qui concerne l'élimination des cyberattaques et de la fraude en ligne, ainsi que de la pédopornographie. Elle couvre également les pratiques opérationnelles des États membres pour ce qui est de la coopération internationale et de l'assistance proposée aux personnes qui sont victimes de la cybercriminalité.

5 Doc. 12109/13 POLGEN 138 JAI 612 TELECOM 194 PROCIV 88 CSC 69 CIS 14 RELEX 633 JAIEX 55 RECH 338 COMPET 554 IND 204 COTER 85 ENFOPOL 232 DROIPEN 87 CYBER 15 COPS 276 POLMIL 39 COSI 93 DATAPROTECT 94.

6 STE nº 185, ouverte à la signature le 23 novembre 2001 et entrée en vigueur le 1er juillet 2004.

7 STE nº 189, ouverte à la signature le 28 janvier 2003 et entrée en vigueur le 1er mars 2006.

L'ordre des visites dans les États membres a été adopté par le groupe GENVAL le 1er avril 2014. La Belgique est l'État membre évalué au cours de cette série d'évaluations. Conformément à l'article 3 de l'action commune, une liste d'experts a été établie par la présidence en vue des évaluations à mener. Les États membres ont désigné des experts possédant une connaissance pratique étendue dans le domaine concerné sur la base d'une demande écrite que le président du groupe GENVAL a adressée aux délégations le 28 janvier 2014.

Les équipes d'évaluation se composaient de trois experts nationaux, assistés de deux fonctionnaires du Secrétariat général du Conseil et d'observateurs. Pour la septième série d'évaluations mutuelles, le groupe GENVAL a approuvé la proposition de la présidence selon laquelle la Commission européenne, Eurojust, Europol/EC3 et l'ENISA devraient être invités en tant qu'observateurs.

Les experts chargés de l'évaluation de la Belgique étaient Monsieur Alain Kleuls de la Police grand-ducale du Luxembourg, Monsieur Rui Batista (PT) et Monsieur Philippe Devred (FR), ainsi que Madame Claire Rocheteau du Secrétariat général du Conseil.

Le présent rapport a été élaboré par l'équipe d'experts avec l'assistance du Secrétariat général du Conseil, sur la base des constatations issues de la visite d'évaluation effectuée en Belgique du 26 au 28 avril 2016, ainsi que des réponses détaillées de la Belgique au questionnaire d'évaluation, accompagnées de ses réponses détaillées aux questions qui ont suivi.

3 QUESTIONS GÉNÉRALES ET STRUCTURES

3.1 Stratégie Nationale en matière de Cybersécurité

Le 21 décembre 2012, le Conseil des ministres a adopté une stratégie nationale de cybersécurité pour la Belgique, dont il a confié la coordination de la mise en œuvre au Premier ministre. Ce projet vise à pourvoir la Belgique d'une stratégie fédérale de sécurité des réseaux et systèmes d'information, dans le respect de la vie privée. Cette cyberstratégie belge a pour objectif d'identifier la cybermenace, d'améliorer la sécurité et de pouvoir réagir aux incidents. Ce projet est né du travail de la plateforme de concertation pour la sécurité de l'information BelNIS (plate-forme de concertation créée par le Conseil des ministres du 30 septembre 2005 et au sein de laquelle se réunissent périodiquement les institutions suivantes: la Commission de la protection de la vie privée, l'Autorité nationale de sécurité, le Service général du renseignement et de la sécurité (SGRS), la Sûreté de l'État, l'Institut belge des services postaux et des télécommunications (IBPT), la Federal Computer Crime Unit (FCCU), le SPF Économie, Fedict, la Banque-Carrefour des Entreprises (BCE), le Centre de crise et le représentant du Collège des procureurs généraux).
Après avoir dressé un état des lieux de la cybermenace en Belgique, trois objectifs stratégiques ont été déterminés dans le cadre de cette stratégie:

- un cyberespace sûr et fiable qui respecte les valeurs et droits fondamentaux de la société moderne;
- la mise en place d'une sécurisation et d'une protection optimales des infrastructures et des systèmes publics critiques contre la cybermenace;
- le développement de capacités propres en matière de cybersécurité.

Pour réaliser ces trois objectifs stratégiques, l'État belge a élaboré plusieurs lignes d'action concrètes:

- une approche centralisée et intégrée de la cybersécurité;
- la création d'un cadre légal;
- le suivi permanent de la cybermenace;
- l'amélioration de la protection contre la perturbation ou la violation des systèmes informatiques;
- le renforcement de la capacité à réagir aux cyberincidents;
- une approche spécifique de la cybercriminalité;
- la contribution à l'élargissement de l'expertise et de la connaissance en cybersécurité;
- la stimulation du développement technologique.

Le texte de cette stratégie est disponible en ligne: http://www.b-ccentre.be.
Il convient également de signaler qu'une nouvelle note-cadre de sécurité intégrale et un nouveau plan national de sécurité sont en cours d'élaboration, dans le cadre desquels la cybercriminalité fera l'objet d'une attention particulière.

Un exemple de bonne pratique dans la lutte contre la cybercriminalité est la Plateforme de concertation: dans le ressort de Gand, deux accords de coopération ont été conclus en matière de criminalité informatique, d'un côté par la province de Flandre orientale, parquets de Gand, Termonde et Audenarde, où cette matière est gérée par le parquet de Termonde et, d'un autre côté, pour la province de Flandre occidentale, où le parquet de Furnes prend en charge cette matière. Les bonnes pratiques sont également transmises au Parquet d'Anvers et de Liège via une circulaire.

Apres la visite d'évaluation, afin de transposer la NIS-directive on a constitue un groupe de travail au sein de CCB qui a comme tache la mise a jour de la cyber stratégie belge.
Il faut aussi mentionner que la note-cadre 2016-2019 de Sécurité intégrale (NCSI)[8] et le Plan national de sécurité 2016-2019[9] sont également disponibles, la cybercriminalité et la cybersécurité étant des priorités dans les deux documents.

[8] http://jambon.belgium.be/sites/default/files/articles/Kadernota%20IV%20FR_DEF.pdf
[9] http://jambon.belgium.be/sites/default/files/articles/PNS_F.pdf

3.2 Priorités nationales en matière de cybercriminalité

Plusieurs actions prioritaires ont été décidées dans la lutte contre la cybercriminalité:

- La création du Centre pour la cybersécurité Belgique (CCB), sous l'autorité du Premier ministre. Une de ses priorités est la gestion efficiente des incidents et des cyberattaques.
- Le renforcement des capacités des Computer Crime unit (CCU) régionales de la Police fédérale judiciaire par des spécialistes dédiés à la lutte contre la cybercriminalité. Ces CCU étaient, jusqu'à présent, principalement spécialisées dans les analyses technico-légales des traces informatiques ainsi que le renforcement de la capacité de la Federal Computer Crime Unit, unité centrale au sein de la Police fédérale judiciaire, par des spécialistes dédiés à la lutte conte les cyberattaques, avec une priorité pour les infrastructures critiques.
- Le renforcement de la capacité du Service général du renseignement et de la sécurité (SGRS) des forces armées, dédié à la protection des sites nationaux.
- La création d'outils légaux adaptés. Cet ensemble de dispositions légales diverses, certaines encore en élaboration, porte sur:
    - les patrouilles sur l'internet, les enquêtes "undercover light";
    - les procédures d'intervention et de saisie;
    - les certifications des enquêteurs spécialisés;
    - les méthodes d'investigations technico-légales;
    - l'extension des recherches dans un système informatique et la problématique du cryptage des données;
    - le piratage (hacking) légal par les forces de police;
    - les problèmes avec les fournisseurs de logiciels de communication (Skype, WhatsApp, etc.).

Il convient de mentionner également les initiatives suivantes:

- la mise en œuvre de la réglementation relative à l'interception sur l'internet;
- la poursuite de la transposition de la directive 2013/40 relative aux attaques contre les systèmes d'information;
- l'optimisation des identifications par un opérateur d'utilisateurs finals de communications électroniques;
- le fait de rendre inaccessibles les sites internet qui contiennent du matériel pédopornographique et de les supprimer plus rapidement : "notice and takedown";
- la création d'une législation réparatrice concernant la conservation des données ("data retention"), celle-ci demeurant un instrument absolument nécessaire et crucial pour les autorités judiciaires.

L'équipe d'évaluation salue les initiatives législatives de la Belgique visant à améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant l'internet, les communications électroniques et les télécommunications, notamment le mémo confidentiel énumérant l'ensemble des activités de recherche sur l'internet, répertoriées et classées suivant le degré d'intrusion dans la vie privée du citoyen, avec indication de leur admissibilité ou non dans la phase proactive et/ou dans la phase réactive.

3.3 Statistiques sur la cybercriminalité

Étant donné que les institutions utilisent chacune des définitions et une méthodologie différentes, il est impossible de comparer et de relier les statistiques qu'elles produisent. L'enregistrement et la classification dépendent aussi du degré de connaissance du policier en la matière. De plus, lors de l'inscription de l'incident, il n'existe pas de possibilité de faire une distinction entre les différents cas de cybercriminalité.

3.3.1 Grandes tendances de la cybercriminalité

Tendances majeures en matière de cybercriminalité

Nous constatons que quelques *modus operandi* connaissent depuis peu un succès grandissant, à savoir:

- les APT (Advanced Persistent Threats ou "menaces persistantes avancées"): le premier cas d'APT qui a été examiné par la police belge était le piratage d'un grand opérateur de télécoms en 2012. Depuis, le nombre de dossiers APT n'a cessé d'augmenter. De plus, on observe l'utilisation, par la criminalité organisée (obtention/achat via l'internet) de (parties de) logiciels malveillants (malwares) sponsorisés par des États (state-sponsored).
- l'extorsion numérique:
  - les "crypto ransomwares" (crypto-rançongiciels) (tels CryptoLocker et CTB-Locker) cryptent des fichiers sur les PC (depuis 2013 et avec un succès grandissant) et demandent un paiement pour récupérer les fichiers;
  - l'extorsion sous la menace de publier des données piratées (depuis 2012).
- les logiciels malveillants sur les appareils mobiles: il ressort que ces logiciels malveillants, qui apparaissent dans les enquêtes récentes, y compris en Belgique, prennent de plus en plus souvent des infrastructures critiques pour cibles (collecte d'informations ou prise de contrôle).

Nous observons aussi que la liste des actes de piratage (connus) d'autorités belges et de figures politiques importantes ne cesse de s'allonger depuis leur début en 2012: le président du Conseil européen, le Premier ministre, un grand opérateur de télécommunications, un professeur (expert en cryptographie), les services publics Affaires étrangères et Économie, des ambassades à Bruxelles, l'Union européenne, des universités, etc.

Enfin, il convient de mentionner l'apparition d'une tendance inquiétante, à savoir la coopération croissante entre des cybercriminels et la criminalité organisée classique: en 2012, pour la première fois en Belgique, a été mise au jour une affaire où il était question du recours à un acte de piratage professionnel dans le milieu de la drogue.

La cybercriminalité par rapport à l'ensemble de la criminalité

Pour les trois dernières années, la criminalité informatique représente entre 1,7 et 2 % de la criminalité globale en Belgique (source: Statistiques policières de criminalité 2000-2014, Police fédérale).

Suite aux premières attaques contre les systèmes de banques en ligne en 2007, une réaction avait été amorcée au niveau du Parquet fédéral, avec l'appui des services d'enquête de la FCCU et du service de lutte contre la criminalité financière organisée (OCDEFO) en collaboration avec le secteur concerné (FEBELFIN et les cinq grandes banques). Nous constatons qu'après avoir été jugulées pendant quelques années, ces attaques ont entraîné, au cours des derniers mois, une nouvelle augmentation des dommages causés.

Par ailleurs, il convient de relever que l'absence de dénonciation des faits aux autorités judicaires, en raison d'un manque de capacité de recensement au niveau des polices locales en ce qui concerne les citoyens (connaissance des phénomènes, dimension internationale, liens avec la criminalité ordinaire, qualification des faits) et en raison d'une crainte de perte de confiance en ce qui concerne les entreprises, explique en grande partie le "chiffre noir" de ce type de criminalité. Les efforts menés, surtout à l'égard des entreprises, pour les inciter à réagir et à dénoncer introduisent, lentement, un changement culturel qui na pas encore apporté les résultats espérés.

3.3.2 Nombre de cas répertoriés de cybercriminalité

Les statistiques sur la cybercriminalité ne sont pas intégrées. Chaque institution/organe les confectionne indépendamment des autres. À l'heure actuelle, il n'est généralement pas possible de lire les statistiques du Parquet en parallèle avec les statistiques policières et les statistiques en matière de condamnations, suspensions et internements. Il existe, en effet, des différences fondamentales au niveau des options méthodologiques et du contenu.

Statistiques policières

Les données de base des statistiques de la criminalité enregistrée sont les procès-verbaux initiaux établis par les services de la police intégrée, structurée à deux niveaux (police locale et police fédérale), qu'il s'agisse d'un délit accompli ou d'une tentative. Les statistiques policières sont disponibles sur http://www.stat.policefederale.be/statistiquescriminalite/.

Statistiques du ministère public

Les analystes statistiques du ministère public peuvent générer des données statistiques provenant de la banque de données centrale du ministère public. Cette banque de données se base sur les enregistrements effectués dans le système informatisé REA/TPI par la section correctionnelle des parquets et greffes près les tribunaux de première instance.

Statistiques des condamnations, suspensions et internements

Ces statistiques peuvent être subdivisées par type d'infraction pénale. Il importe de savoir à cet égard qu'un jugement prononcé par un tribunal et inscrit pour un individu dans un bulletin de condamnation peut porter sur plusieurs infractions pénales. En outre, un individu peut être condamné plusieurs fois par an et avoir, par conséquent, plusieurs bulletins de condamnation par an. Le nombre total de condamnations, de suspensions ou d'internements par infraction pénale est donc beaucoup plus élevé que le nombre total de bulletins de condamnation par juridiction ou par ressort et que le nombre total de condamnés.

Si des chiffres fiables et représentatifs sont disponibles pour les années 1995-2005, les données chiffrées sur les condamnations relatives aux années 2006-2012 sont une sous-évaluation de la réalité en raison de l'arriéré dans l'enregistrement des bulletins de condamnation au Casier judiciaire central.

Statistiques produites par le CERT

Le CERT ne rassemble pas les chiffres relatifs à la cybercriminalité, mais plutôt en matière de communications d'incidents, dont il est avéré, ces dernières années, que beaucoup sont de plus en plus souvent liés à la cybercriminalité.

Après filtrage, ces incidents sont examinés en interne et classifiés sur la base d'une taxonomie. Cette taxonomie sera bientôt revue, pour améliorer la transmission des données et répondre plus efficacement aux attentes. Cette taxonomie tiendra compte aussi bien de l'impact de l'incident que de son origine (root-cause).

Ces chiffres sont publiés sur https://www.cert.be/fr/chiffres, bien que certaines parties ne soient pas communiquées aux tiers.

Il existe cependant une collaboration avec la Federal Computer Crime Unit et d'autres services peuvent également être informés en cas d'augmentation anormale d'incidents de même nature.

Il est également question d'effectuer une transmission de données mensuelle à haut niveau vers l'autorité judiciaire axée sur la détection de phénomènes de cybercriminalité, mais cette procédure n'est pas encore formalisée.

Statistiques policières de criminalité

Année	Nombre d'infractions de criminalité informatique: art. 210 *bis* (faux en informatique), art. 504 *quater* (fraude en informatique), art. 550 *bis* (hacking) et art. 550 ter (sabotage informatique)
2005	4.322
2006	5.736
2007	7.741
2008	9.112
2009	11.668
2010	14.476
2011	15.763
2012	22.023
2013	18.002
2014	16.561

Source: Statistiques policières de criminalité 2000-2014, Police fédérale

Les statistiques de 2015, ainsi qu'une mise a jour des autres chiffres sont disponibles à l'adresse suivante:
http://www.stat.policefederale.be/assets/pdf/crimestat/nationaal/rapport_2016_trim1_nat_belgique_fr.pdf.

Statistiques du Ministère public

Nombre d'infractions de criminalité informatique						
	2013		2014		Total	
	N	%	N	%	n	%
Faux en informatique	1.024	4,79	1.538	7,16	2.562	5,97
Fraude en informatique	16.890	78,94	15.962	74,28	32.852	76,60
Hacking	662	3,09	721	3,36	1.383	3,22
Sabotage informatique	778	3,64	222	1,03	1.000	2,33
Refus de fournir une collaboration à une demande de coopération (dans le cadre d'une recherche dans un système informatique, p.ex. renseignement sur le fonctionnement du système) émise par le juge d'instruction ou faire obstacle à un ordre de recherche dans le système informatique émis par le juge d'instruction	3	0,01	3	0,01	6	0,01
Faux en informatique, y compris fausses cartes bancaires.	393	1,84	443	2,06	836	1,95
Autres	1.646	7,69	2.600	12,10	4.246	9,90
Total	21.396	100.00	21.489	100,00	42.885	100,00

Statistiques des condamnations, suspensions et internements

Comme mentionné dans la réponse à la question 6, les données chiffrées relatives aux années 2006-2012 portant sur les condamnations sont une sous-évaluation de la réalité et ne sont donc pas souvent utilisés, vous les trouverez ci-dessous:

Année	Nombre d'infractions de criminalité informatique: art. 210 *bis* (faux en informatique), art. 504 *quater* (fraude en informatique), art. 550 bis (hacking) art. 550 *ter* (sabotage informatique) du Code Pénal
2005	369
2006	441
2007	528
2008	464
2009	519
2010	561
2011	628
2012	743
2013	624

Source: Service de la Politique criminelle du SPF Justice

Statistiques du CERT.be

Ci-dessus le nombre d'incidents rapportés au CERT.be de 2010 à 2014:

	2010	**2011**	**2012**	**2013**	**2014**
Total reports received	2135	2609	3866	6678	10812
Total of them that were incidents	**1389**	**1494**	**1981**	**4070**	**9866**
Incidents related to worms and viruses	13,0 %	4,6 %	6,0 %	22,0 %	29,5 %
Scan incidents	5,0 %	26,1 %	29,0 %	20,0 %	30,5 %
System incidents	24,0 %	24,1 %	21,0 %	14,5 %	3,5 %
Phishing incidents	8,0 %	14,7 %	17,0 %	14,0 %	5,5 %
Incidents related to spam	7,0 %	14,8 %	4,5 %	13,0 %	5,0 %
Other incidents	10,0 %	3,1 %	11,0 %	10,5 %	3,5 %
Incidents reporting vulnerabilities	0 %	0,7 %	2,0 %	3,0 %	21,0 %
Incidents with denial-of service attacks	0 %	2,4 %	1,5 %	1,5 %	0,5 %
Incidents/questions about internet security related topics	1,0 %	4,3 %	4,0 %	1,0 %	0,5 %
Incidents with accounts	32,0 %	5,2 %	4,0 %	0,5 %	0,5 %

D'autre part, des sources "automatisées" (capteurs) rapportent automatiquement des incidents; pour le premier semestre de 2014, ce système a permis d'en relever plus de 750 000. L'analyse de ces sources sur la base d'une nouvelle méthodologie est actuellement en cours. En 2013, l'analyse a permis de déterminer qu'une grande partie de ces incidents était liée à des ordinateurs membres d'un "botnet".

Les statistiques de la Police, du Ministère public et des condamnations ne permettent pas de fournir une idée précise du nombre et de la nature des cyberinfractions constatées et/ou sanctionnées, ni du nombre de personnes ayant fait l'objet d'enquêtes, de poursuites et de condamnations pour des actes de cybercriminalité.

Les statistiques du CERT vont déjà plus dans le détail en classifiant les infractions sur la base d'une taxonomie. Pour améliorer les statistiques, cette taxonomie est revue afin de tenir compte aussi bien de l'impact de l'incident que de son origine.

Comme de nombreux autres pays, la Belgique se heurte à la difficulté de quantifier, avec un niveau de précision satisfaisant, un phénomène criminel de plus en plus large et qui recouvre à la fois des infractions dont la définition légale identifie la dimension cybercriminelle et des infractions de droit commun commises au moyen des technologies de l'information.

L'équipe d'évaluation salue l'effort engagé par la Belgique afin de changer le système informatique de manière à relier les différentes bases de données des diverses entités qui relèvent des statistiques. Le but est de fournir des chiffres depuis le début de l'incident jusqu'à la condamnation du prévenu.

Le "chiffre noir" de la cybercriminalité, c'est-à-dire l'absence de dénonciation des faits aux autorités répressives, est élevé. Selon les autorités belges, la raison en est à la fois un manque de capacité de recensement au niveau des polices locales en ce qui concerne les citoyens (connaissance des phénomènes, dimension internationale, liens avec la criminalité ordinaire, qualification des faits) et une crainte de perte de confiance en ce qui concerne les entreprises.

3.4 Dotations budgétaires nationales pour la prévention de la cybercriminalité et la lutte contre celle-ci et contribution financière de l'UE

Il n'y a pas d'approche globale en ce qui concerne les budgets alloués à la lutte contre la cybercriminalité. La Belgique a fourni les renseignements suivants:

- La Police fédérale dispose d'un budget d'investissement distinct qui est utilisé pour l'achat de matériel d'enquête TCI spécifique en matière scientifique/forensique pour les "Computer Crime Units" (FCCU + RCCU). En 2015, ce budget s'élevait à 511 333 €.
- Le Centre pour la cybersécurité Belgique (CCB), créé depuis le 17/8/2015, s'est vu octroyer en 2015 un budget d'environ 719 000 euros pour assurer son fonctionnement et sa mise en place. Ce budget n'est donc pas spécifiquement attribué à la lutte contre la cybercriminalité. Le centre fait appel a des provisions interdépartementales pour financer les projets de cybersécurité.
- Dans le cadre de BRAIN-be (Belgian Research Action through Interdisciplinary Networks, qui intègre les instruments de financement de la recherche fédérale) un budget de 684 731 € a été libéré pour le projet "Mesure du coût et de l'impact de la cybercriminalité en Belgique". Cette recherche multidisciplinaire est cependant en cours de réalisation (du 1er décembre 2013 au 28 février 2018). Menée sur une période de quatre ans, la recherche donnera une vue plus globale et scientifiquement étayée de l'impact de la cyber menace, grâce à un modèle spécifique au pays permettant de mesurer le coût et l'impact de la cybercriminalité. La recherche fournira également des directives et des orientations stratégiques pour les décideurs politiques sur la façon de faire progresser la mise en œuvre des principes contenus dans la stratégie belge de la cybersécurité.

3.5 Conclusions

La Belgique a une stratégie nationale de cybersécurité, qui a été adoptée le 21 décembre 2012. Cette stratégie (http://www.b-ccentre.be) se détermine par trois objectifs:

- un cyberespace sûr et fiable qui respecte les valeurs et droits fondamentaux de la société moderne;
- la mise en place d'une sécurisation et d'une protection optimales des infrastructures et systèmes publics critiques contre la cybermenace;
- le développement de capacités propres en cybersécurité et plusieurs lignes d'action concrètes:
- une approche centralisée et intégrée de la cybersécurité;
- la création d'un cadre légal;
- le suivi permanent de la cybermenace;
- l'amélioration de la protection contre la perturbation ou la violation des systèmes informatiques;
- le renforcement de la capacité de réagir aux cyberincidents;
- une approche spécifique à la cybercriminalité;
- la contribution à l'élargissement de l'expertise et des connaissances en matière de cybersécurité;
- la stimulation du développement technologique.

Le plan national de sécurité 2016-2019 présenté après la visite fait figurer la cybersécurité parmi les 10 principaux phénomènes de sécurité.

L'équipe d'évaluation considère important que le rôle d'implémentation et de coordination soit assuré par le Centre pour la cybersécurité Belgique (CCB) fondé en octobre 2014. Le CCB relève de l'autorité du Premier ministre. A l'époque de l'évaluation, le CCB était en cours de création. Il est donc important d'assurer le recrutement de spécialistes et leur fidélisation à long terme.

L'équipe d'évaluation a constaté qu'il existait un projet de centralisation et de recherche dans le domaine de la cybercriminalité et de la cybersécurité initié par l'université KU Leuven en 2011: le B-CCENTRE (Belgian Cybercrime Centre of Excellence). Ce projet n'est plus soutenu. Cette entité avait pour rôle de rassembler les acteurs principaux, de soutenir les échanges d'informations dans le domaine de la cybercriminalité, de proposer des formations et d'exercer déjà certaines actions de la stratégie nationale en cybersécurité. Bien que le CCB soit appelé à reprendre les activités du B-CCENTRE, il convient que l'expertise déjà existante soit soutenue et intégrée. Après la visite d'évaluation Le CCB a démarré les démarches nécessaires, ensemble avec le SPF Intérieur, afin de demander les subsides nécessaires auprès de l'UE pour la reprise du B-CCentre. Un appel à candidature va être lancé auprès des Universités pour gérer les subsides.

L'équipe d'évaluation constate un manque de communication entre les acteurs impliqués (CCB et B-CCENTRE). Il faudrait donc rassembler les efforts déjà réalisés.

Concernant les statistiques, il faudra définir des standards et des normes pour pouvoir comparer les statistiques des différentes autorités. Cette recommandation vaut pour tous les États membres et non seulement pour la Belgique. Les dispositifs actuels de comptage des infractions ne permettent pas d'appréhender quantitativement la cybercriminalité constatée, tant dans son ensemble que par type d'infraction. Ils permettent seulement de constater des tendances globales. Le chiffre noir de la cybercriminalité en Belgique est dû à un défaut de signalement systématique des infractions aux autorités compétentes.

L'équipe d'évaluation considère que la Belgique devrait revoir les règles de financement - les moyens et les ressources humaines - applicables à la lutte contre la cybercriminalité, en particulier en ce qui concerne l'acquisition de dispositifs techniques ou de logiciels et les rémunérations des experts.

Ce problème se pose encore davantage au sein de la Police fédérale, car les policiers chargés de la lutte contre la cybercriminalité au niveau central sont moins bien rémunérés qu'au niveau régional.

4 STRUCTURES NATIONALES

4.1 Système judiciaire (poursuites et juridictions)

4.1.1 Structure interne

Les institutions responsables de la prévention et de la lutte contre la criminalité sont, en synthèse:

- Police fédérale;
- Ministère public;
- Centre pour la cybersécurité Belgique (CCB);
- Federal Cyber Emergency Team (CERT.be): financé par la Chancellerie du Premier ministre et le CCB, le CERT.be est composé d'un coordinateur, d'un responsable communication/presse, d'un gestionnaire système dédié et de cinq analystes en sécurité informatique. Un poste de coordinateur adjoint et trois postes d'analystes sont encore vacants;
- Un soutien de BELNET est fourni en matière juridique, de gestion de ressources humaines et administrative ainsi qu'un support technique pour les infrastructures;
- Service public fédéral Technologie de l'information et de la communication (Fedict);
- Institut belge des postes et télécommunications (IBPT);
- Service de renseignement des Forces armées (SGRS);
- Commission de la vie privée.

Le ministère public occupe une position centrale au sein de la justice belge. Il est composé de magistrats de parquet qui agissent au nom de l'État et défendent les intérêts de la société. Ils poursuivent les contrevenants devant le tribunal, dirigent l'enquête pénale, recherchent les auteurs et réclament au tribunal des peines contre les suspects.

Le ministère public se compose de diverses entités. Près les tribunaux de première instance (niveau provincial), les tâches sont assurées par les parquets du procureur du Roi. Il existe 12 arrondissements judiciaires avec 14 parquets. A ce niveau, il n'existe pas de spécialisation en matière de cybercriminalité, tous les procureurs étant compétents à cet égard. Tous les magistrats devraient avoir des connaissances de base en matière cybercriminalité, selon le vœu du ministère public. Il faut préciser que chaque parquet dispose d'un magistrat de référence en matière de cybercriminalité.

Au niveau de la Cour d'appel, le ministère public est représenté par les parquets généraux. Il existe 5 procureurs généraux qui forment ensemble le Collège des procureurs généraux.

Au niveau fédéral, le ministère public est représenté par 1 procureur fédéral qui traite les phénomènes et faits complexes qui dépassent les limites des arrondissements - tels que la traite des êtres humains, le terrorisme, la criminalité organisée et le blanchiment. Il est également chargé de faciliter la coopération internationale et de surveiller le fonctionnement de la Police fédérale.

En ce qui concerne le domaine de la cybercriminalité, il est placé sous la responsabilité du procureur général d'Anvers, en coordination avec le procureur fédéral.

Le domaine de la cybercriminalité fait partie du domaine de compétence de la police fédérale (FCCU). Tous les dossiers concernant des attaques contre des sites critiques et sensibles sont centralisés auprès de la FCCU tandis que les autres attaques d'envergure régionale sont traitées par les RCCU.

La réunion avec les différents acteurs a révélé que les modalités d'attribution des dossiers ne sont pas claires et que les décisions semblent être prises au cas par cas. Il n'existe pas de hiérarchie entre la FCCU et les RCCU.

4.1.2 Capacités disponibles et obstacles à l'aboutissement des poursuites

La formation de base en cybercriminalité - qui est obligatoire pour les stagiaires judiciaires de deuxième année - vise à sensibiliser les magistrats à la criminalité informatique.

La formation spécialisée en cybercriminalité - qui s'adresse particulièrement aux magistrats, aux stagiaires judiciaires et aux juristes de parquet - permet d'acquérir une connaissance approfondie sur l'utilisation des médias sociaux dans les enquêtes proactives et réactives pénales, l'utilisation des méthodes de recherche particulières dans un entourage virtuel, la coopération internationale en matière pénale (en particulier avec les USA), plus particulièrement en ce qui concerne les traces et les preuves numériques, ainsi que sur les compétences et juridictions territoriales dans le cyberespace.

De plus, un réseau d'expertise a été créé au sein du Collège des procureurs généraux.

En 2008, le Collège des procureurs généraux, définissant la politique en matière de cybercriminalité, a pris la décision qu'il devait exister au moins un magistrat de référence au niveau du parquet, du parquet général et du parquet fédéral. Il est attendu que ces magistrats se familiarisent avec la matière et suivent les formations spécialisées.

Le Collège des procureurs généraux s'est doté d'un réseau d'expertise en cybercriminalité regroupant des représentants du parquet fédéral, du parquet général, du parquet de première instance, de la Police fédérale (FCCU), du CCD et, sur invitation, des juges d'instruction pour accroître l'expertise du ministère public en la matière, faciliter la communication et la documentation et faciliter les contacts avec les institutions en dehors du Ministère public. Ce réseau d'expertise n'a pas de tâches opérationnelles (enquêtes).

Seuls les magistrats des parquets sont chargés de la recherche et de la poursuite des infractions. Ils peuvent charger un juge d'instruction de mener l'enquête.

En général c'est la police (locale ou fédérale) qui accomplit les actes de police judiciaire et fait rapport aux parquets.

Les principaux obstacles constatés par les autorités belges à l'aboutissement de poursuites contre des actes de cybercriminalité sont les suivants:

- impossibilité d'intercepter les communications Voice over IP;
- problématique du cryptage (volumes cryptés)
- absence de réglementation claire et absence de directives (européennes) concernant la juridiction des opérateurs qui fournissent activement des services en Europe;
- problématique de la conservation de données;
- utilisation d'outils empêchant l'identification (TOR);
- utilisation de l'Internet caché (DARKNET);
- lenteur de l'entraide judiciaire, indépendamment de la volonté des autorités;
- manque et absence de déclaration d'incidents et de plaintes de la part des victimes;
- moyens répressifs inadaptés pour traiter les phénomènes de masse;
- enquêtes longues et complexes, nécessitant souvent des coopérations internationales;
- manque d'homogénéité des législations nationales;
- surcharge des services spécialisés;
- volume des données à analyser;
- manque de capacité qualifiée.

Les autorités judiciaires (parquet et juridictions) qui doivent examiner les dossiers de cybercriminalité ne sont pas toujours sensibles aux enjeux; cela est dû à une méconnaissance des mécanismes qui sont par ailleurs complexes et à un manque de formation/spécialisation dans le domaine de la cybercriminalité.

4.2 Autorités répressives

Les services spécialisés dans la répression de la cybercriminalité sont les suivants:

- La Federal Computer Crime Unit (FCCU), unité centrale, dépendant de la Direction de la lutte contre la criminalité grave et organisée (DJSOC), est en charge des enquêtes liées aux cyberattaques contre les infrastructures critiques, aux cyberattaques et autres enquêtes sur la cybercriminalité en appui aux Computer Crime Units régionales (RCCU). Avec un effectif organique de 44 enquêteurs, la FCCU comporte entre autres une équipe de 8 membres spécialisée pour réagir judiciairement aux cyberincidents et une équipe de 6 membres dédiée à la collecte et au traitement de l'information;
- Les Regional Computer Crime Units, unités régionales, réalisent les enquêtes relatives aux cyberattaques et fournissent l'appui technico-légal dans les enquêtes de criminalité non spécifiques. Les effectifs des RCCU sont déterminés par les directeurs régionaux de la Police judiciaire fédérale et varient de 3 à plus de 30 personnes, qui ont toutes suivi la formation de base "enquêteur CCU".
- Au sein du Service public fédéral Économie, une section d'enquêteurs est chargée des poursuites relatives aux infractions aux lois économiques commises par l'utilisation de l'internet;
- Au sein du Service public fédéral Finances, le Belgian Internet Service Center (BISC) regroupe une section d'enquêteurs en charge des poursuites relatives aux fraudes financières et de la détection de la mise en place de mécanismes de fraude par l'utilisation de l'internet. Ce service réalise également des recherches technico-légales.

Les premiers intervenants sur le lieu du crime sont les agents de la police locale, chargés de geler le lieu et de sauvegarder les supports TCI. Suivant le responsable de la FCCU, le réseau de premiers intervenants est encore à créer.

Concernant les effectifs, la FCCU compte 28 personnes au lieu de 44 (effectif théorique). Les RCCU emploient 180 personnes au lieu des 260 prévues.

Un point critique invoqué par les responsables est qu'actuellement, la Police (FCCU et RCCU) compte seulement 7 ou 8 personnes ayant la capacité opérationnelle de faire une expertise spécialisée. De plus, les unités souffrent d'une surcharge de travail et d'un arriéré de traitement important.

Un autre point relevé lors de la visite est que le spécialiste est rarement impliqué dans l'affaire et qu'il ignore souvent ce que l'enquêteur recherche.

L'inexistence d'une répartition claire des missions entre les différents acteurs (FCCU et RCCU) a été mentionnée.

Les mêmes problèmes ont été relevés par les différentes RCCU, à savoir: manque de personnel, moyens insuffisants, manque de formations, retards inacceptables dans le traitement des dossiers, procédures de recrutement non adaptées. Le budget ne suffit même pas pour renouveler les licences existantes des logiciels utilisés pour l'exploitation des supports informatiques soumis à un examen forensique.

Le budget alloué pour des formations externes en cybercriminalité est de seulement 3000 € pour l'ensemble de la Police judiciaire.

4.3 Autres services et partenariat public-privé

En sus du Parquet fédéral et de la Police judiciaire fédérale, s'agissant de la détection, de la prévention et de la réaction en cas de faits de cybercriminalité, les acteurs suivants peuvent être appelés à intervenir, dans le cadre de leurs missions fixées par la loi:

- Les cyberexperts du Service général du renseignement et de la sécurité (SGRS) des Forces armées, dépendant du Service public fédéral Défense

Ces experts participent également aux exercices nationaux et internationaux.

- Le CERT.be

Le CERT.be est l'équipe fédérale d'intervention d'urgence en sécurité informatique, gérée par CCB, à la demande du SPF Chancellerie du Premier ministre. Le CERT.be travaille au sein d'un réseau mondial d'experts en sécurité informatique et s'attaque aux problèmes de sécurité sur l'internet à travers la coordination, l'information et la sensibilisation.

Les professionnels TCI peuvent s'adresser gratuitement et en toute confidentialité au CERT.be afin de signaler des problèmes informatiques (piratage de données et d'infrastructures de réseau, hameçonnage (phishing), cyberattaques, etc.). Le CERT.be donne des conseils pour régler l'incident aussi rapidement que possible et coordonne les actions de toutes les entreprises ou organisations impliquées.

Le CERT.be donne également des conseils aux particuliers et aux entreprises afin de sécuriser leur utilisation de l'internet. Les entreprises trouvent ces informations sur www.cert.be, tandis que le grand public est invité à consulter le nouveau site www.safeonweb.be.

Le CERT.be participe aux exercices nationaux et internationaux.

- La Sureté de l'État

La Sureté de l'État constitue le service de renseignement belge; elle agit, sous le contrôle du Comité R qui rend compte au Premier ministre.

- Les autorités sectorielles compétentes en matière d'infrastructures critiques

Les exploitants d'infrastructures critiques sont tenus d'élaborer et de mettre en œuvre un plan de sécurité interne contenant des mesures de sécurité permanentes (en tout temps) et graduelles (en fonction du niveau de la menace). Ces mesures couvrent tant la sécurité physique de l'infrastructure que la sécurité des réseaux et systèmes informatiques.

Les autorités sectorielles ont la possibilité de détailler des mesures spécifiques pour ce qui concerne les infrastructures critiques relevant de leur compétence et sont chargées d'organiser un contrôle régulier de ces plans.

En Belgique, les cinq secteurs critiques existant actuellement sont les suivants:

- le secteur de l'énergie (autorité sectorielle: le ministre de l'Énergie);
- le secteur des transports (autorité sectorielle: le ministre de la Mobilité);
- le secteur des finances (autorité sectorielle: la Banque nationale de Belgique);

- le secteur des communications électroniques (autorité sectorielle: l'Institut belge des services postaux et des télécommunications, par délégation du ministre ayant les communications électroniques dans ses attributions);
- le secteur "spatial" (limité aux stations au sol dans le cadre des programmes Galileo et EGNOS) (autorité sectorielle administrative: la Haute Représentation belge pour la politique spatiale et autorité chargée des contrôles: l'Autorité nationale de sécurité).

Le Centre de crise est chargé de la politique de coordination en matière d'infrastructure critique.

- L'Institut belge des postes et télécommunications (IBPT)[10]

L'IBPT est le régulateur en matière de télécommunications, et donc en matière de contrôle des fournisseurs d'accès à l'internet, mais également des dispositifs radio (wi-fi, etc.).

- Le Fedict, Service public fédéral Technologie de l'information et de la communication
- Le Service public fédéral Économie (SPF Économie)
- La cellule d'enquête BISC au sein du Service public fédéral Finances (SPF Finances)
- Depuis fin 2015, le CCB, mieux décrit ci-dessous.

[10] http://www.ibpt.be/fr.

Dans le cadre de la détection, de la prévention et de la réaction en cas de faits de cybercriminalité, les acteurs suivants peuvent être appelés à intervenir:

- Les cyberexperts du Service général du renseignement et de la sécurité (SGRS) des Forces armées, dépendant du Service public fédéral Défense. Ces experts participent également aux exercices nationaux et internationaux.
- Le CERT.be: Le CERT.be est l'équipe fédérale d'intervention d'urgence en sécurité informatique, gérée par Belnet, le réseau scientifique national belge, à la demande du SPF Chancellerie du Premier ministre. Le CERT.be participe aux exercices nationaux et internationaux.
- La Sureté de l'État constitue le service de renseignement belge.
- Les autorités sectorielles compétentes en matière d'infrastructures critiques: les exploitants d'infrastructures critiques sont tenus d'élaborer et de mettre en œuvre un plan de sécurité interne contenant des mesures de sécurité permanentes (en tout temps) et graduelles (en fonction du niveau de menace). Ces mesures couvrent tant la sécurité physique de l'infrastructure que la sécurité des réseaux et systèmes informatiques.
- L'Institut belge des postes et télécommunications (IBPT): l'IBPT est le régulateur en matière de télécommunications, et donc en matière de contrôle des fournisseurs d'accès à l'internet, mais également des dispositifs radio (wi-fi, etc.).
- Le Fedict, Service public fédéral Technologie de l'information et de la communication
- Le Service public fédéral pour l'économie (SPF Économie)
- La cellule d'enquête BISC au sein du Service public fédéral Finances (SPF Finances)
- Le CCB depuis 2015.

Dans le cadre de la coopération avec différentes entreprises privées ayant leur siège dans un État tiers, cela se fait sur une base négociée et volontaire, mais avec des fortunes diverses. Il y a des accords "individuels" avec certaines grandes sociétés privées, mais cela reste un exercice d'équilibriste. Ces sociétés privées doivent aussi répondre à la législation nationale qui, parfois, interdit la transmission de données à un pays tiers. Le cas échéant, nous suivons la voie des commissions rogatoires internationales, procédure lourde et lente.

Les entreprises privées peuvent être soumises à des mesures de contrainte telles les perquisitions. Par ailleurs, il peut être demandé aux fournisseurs de services de télécommunications de prêter leur concours sous peine de sanctions en cas d'absence de collaboration (cf. affaire Yahoo).

Concernant les ressources destinées au renforcement de la coopération avec le secteur privé, il convient de mentionner qu'au niveau de la Police judiciaire fédérale, l'approche "intégrale et intégrée" de la nouvelle stratégie soutient le renforcement de la coopération avec le secteur privé. Les ressources qui y sont consacrées se mesurent uniquement en ressources humaines, aucune ressource financière n'étant disponible.

La collaboration avec le monde universitaire, débutée avec la création du centre d'excellence B-CCENTRE en 2011, a permis d'intégrer les besoins de la lutte contre la cybercriminalité exprimés par les autorités judiciaires (par la participation de l'Institut de formation judiciaire) et les autorités policières (par la participation de la FCCU) aux projets réalisés en matière de formations, de recherche et de développement et de prévention (surtout à l'intention des entreprises)[11].

[11] https://www.b-ccentre.be/.

La collaboration avec la Fédération des entreprises de Belgique (FEB) est active depuis plus de dix ans dans la réalisation de normes, l'élaboration de guides de bonnes pratiques et les campagnes de sensibilisation et de prévention (surtout vers les entreprises).

Ces deux partenaires (B-CCENTRE et FEB), ont également pu compter sur la retour d'expérience de la Police fédérale dans l'élaboration du Guide belge de la cybersécurité. Ce guide peut être téléchargé en anglais, français et néerlandais.

Il convient enfin de mentionner l'investissement dans la participation aux initiatives au niveau international en matière de formation (ECTEG) et de recherche et développement, tel que le projet FREETOOLS ayant pour résultat la mise à la disposition des enquêteurs spécialisés, par Europol/EC3, d'outils de recherches technico-légales gratuits.

En fonction des phénomènes, il est possible d'initier des coopérations ad hoc . Ainsi, depuis les attaques contre les systèmes des banques en ligne, la collaboration avec le secteur, via FeBelFin, et les cinq grandes entités bancaires belges, en collaboration avec la Banque nationale (précédemment avec la CBFA) a permis de diminuer les dommages encourus par les banques et les particuliers, et d'établir de nouvelles normes de sécurité imposées par l'organe régulateur (la Banque nationale).

4.4 Coopération et coordination au niveau national

Le Centre pour la cybersécurité Belgique (CCB) a été créé en 2015 et devra être opérationnel en 2016.

Il a dans ses attributions de:

- superviser, coordonner et assurer la mise en œuvre de la stratégie belge en la matière;
- gérer, par une approche intégrée et centralisée, les différents projets relatifs à la cybersécurité;
- assurer la coordination entre les services et autorités concernés mais aussi entre les autorités publiques et le secteur privé ou le monde scientifique;
- formuler des propositions pour l'adaptation du cadre légal et réglementaire en matière de cybersécurité;
- assurer la gestion de crise en cas de cyberincident, en coopération avec le Centre de coordination et de crise du gouvernement;
- élaborer et diffuser des standards, directives et normes de sécurité pour les différents types de systèmes informatiques des administrations et organismes publics et veiller à leur mise en œuvre;
- coordonner la représentation belge dans les enceintes internationales sur la cybersécurité, le suivi des obligations internationales et la présentation du point de vue national en la matière;
- coordonner l'évaluation et la certification de la sécurité des systèmes d'information et de communication;
- informer et sensibiliser les utilisateurs des systèmes d'information et de communication.

À terme, le CCB déterminera, avec les acteurs et autorités compétents, des procédures pour faciliter la gestion des incidents et la communication entre ces différents acteurs en cas d'incidents ou d'attaques. Le CCB jouera un rôle de premier plan dans la coordination de ces autorités et acteurs compétents dans le cadre de la lutte contre les cybermenaces.

Le BElgium Network Information Security (BELNIS) permet aux institutions fédérales de se concerter sur les enjeux nationaux de sécurité de l'information et sur les initiatives souhaitables en la matière. BELNIS est la seule instance permettant aux acteurs de terrain de se rencontrer. En sont membres permanents: la Cellule stratégique du ministre/secrétaire d'État en charge de l'informatisation de l'État, la Commission de la protection de la vie privée, l'Autorité nationale de sécurité, la Banque Carrefour de la Sécurité sociale, l'Institut belge des postes et des télécommunications, la Federal Computer Crime Unit, le Service général du renseignement et de la sécurité (SPF Défense), le SPF Économie, Fedict, le Centre de crise (SPF Intérieur), la Sûreté de l'État, le Service public de programmation de la Politique scientifique, le SPF Justice, le Parquet fédéral, le Collège des procureurs généraux et l'OCAD-OCAM (évaluation de la menace). BELNIS peut inviter des experts extérieurs, le cas échéant. Le groupe de travail organise ses réunions en fonction de ses besoins.

BELNIS ne joue pas de rôle dans la gestion opérationnelle des incidents de sécurité, mais ceux-ci alimentent évidemment la réflexion des experts présents.

Le Parquet fédéral: pour la partie répressive, l'organisation entre les différentes autorités nationales est assurée, pour chaque enquête, par le procureur du Roi et/ou le juge d'instruction saisi pour les faits incriminés. Dans les cas d'attaques sur des infrastructures critiques, le Parquet fédéral coordonne les actions.

Lors de la visite, le CCB était en train de se positionner et en cours de recrutement de personnel. Son rôle n'est pas encore tout à fait défini et le flux d'informations en cas d'incident n'est pas non plus clairement défini. L'équipe d'évaluation se demande également qui déclenchera la crise lors d'un incident majeur. L'intégration du monde universitaire nous semble difficile, vu que le projet B-CCENTRE de l'université a été abandonné.

4.4.1 Obligations légales ou de principe

Concernant la déclaration d'infractions cybercriminelles, c'est la procédure pénale commune qui est suivie. D'une manière générale, le droit belge n'oblige pas les particuliers ou les entreprises à signaler les incidents ou infractions de cybercriminalité.

Pour ce qui concerne les infrastructures critiques, l'article 14 de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques impose aux exploitants de ces dernières de notifier aux services compétents tout événement se produisant, qui serait de nature à menacer la sécurité (physique ou informatique) de son infrastructure.

Il n'y a pas d'obligation légale mais un centre (Federal Cyber emergency team) a été mis en place par l'État pour centraliser les informations et assister les entreprises (https://www.cert.be/fr).

Actuellement, le CCB, en collaboration avec tous les acteurs concernés (FCCU/CCU/CERT/SGRS, etc.), est en train de rédiger une procédure de gestion des cyberincidents nationaux et des cybercrises, avec une définition claire des processus à respecter et des rôles et responsabilités de chaque acteur.

Après la visite d'évaluation un cyber plan national d'urgence a été approuvé par le Conseil national de sécurité, sous réserve de l'approbation du Conseil des Ministres. Ce plan donne des indications sur le procédures à suivre et les mesures de protection a prendre au cas d'évènements de cybersécurité. Trois niveaux sont identifiés: les situations nationales de crise en matière de cybersécurité, les incidents en matière de cybersécurité et les petits incidents en matière de cybersécurité.

La FCCU de la Police fédérale participe au groupe de travail "Internet banking security", qui se penche sur les vulnérabilités et menaces de la fraude à la banque en ligne. Dans le cadre de l'optimalisation de la Police fédérale, il a été décidé qu'il n'y a pas de suivi national concernant les autres formes de fraude à la carte de paiement, ces dossiers étant gérés par les services de la Police fédérale des arrondissements, qui ont également de bons contacts avec l'industrie, mais plutôt au cas par cas.

Des méthodes de gel de données peuvent être ordonnées aux opérateurs en application de l'article XII.17 de la législation économique. S'ils constatent l'existence d'une infraction ou si celle-ci est portée à la connaissance de leurs services, ils ont le devoir de préserver toutes les données et de les mettre à la disposition du procureur du Roi.

4.4.2 Ressources affectées à l'amélioration de la coopération

Au niveau de la Police judiciaire fédérale, le renforcement de la coopération avec le secteur privé est soutenu. Les ressources qui y sont consacrées se mesurent uniquement en ressources humaines, aucune ressource financière n'étant disponible.

La collaboration avec le monde universitaire, entamée lors de la création du centre d'excellence B-CCENTRE en 2011, a permis d'intégrer les besoins de la lutte contre la cybercriminalité, exprimés par les autorités judiciaires et les autorités policières, aux projets réalisés en matière de formations, de recherche et de développement et de prévention.

La collaboration avec la Fédération des entreprises de Belgique (FEB) est active depuis plus de dix ans pour la réalisation de normes, l'élaboration de guides de bonnes pratiques et les campagnes de sensibilisation et de prévention (surtout à l'intention des entreprises).

Il convient enfin de mentionner l'investissement dans la participation aux initiatives au niveau international en matière de formation (ECTEG) et de recherche et développement telles que le projet FREETOOLS ayant pour résultat la mise à la disposition des enquêteurs spécialisés, par Europol/EC3, d'outils de recherches technico-légales gratuits.

En fonction des phénomènes, des coopérations ad hoc peuvent être initiées. Ainsi, depuis les attaques sur les systèmes des banques en ligne, la collaboration avec le secteur, via FeBelFin, et les cinq grandes entités bancaires belges, en collaboration avec la Banque nationale (précédemment avec la CBFA) a permis de diminuer les dommages encourus par les banques et les particuliers, et d'établir de nouvelles normes de sécurité imposées par l'organe régulateur (la Banque nationale).

4.5 Conclusions

La FCCU est le service de police spécialisé dans la lutte contre la cybercriminalité au niveau fédéral, en charge des grandes enquêtes dans ce domaine. Au niveau régional, il existe des structures spécialisées de la police fédérale, les RCCU. L'équipe d'évaluation a constaté que la police locale a aussi des compétences en la matière et qu'elle a développé aussi quelques unités spécialisées, des LCCU. L'équipe d'évaluation a constaté un certain malaise concernant le manque de clarté et de hiérarchie dans le cadre des structures de la Police fédérale et des polices locales.

L'équipe d'évaluation est consciente que des preuves numériques sont requises pour un grand nombre d'infractions. Étant donné que celles-ci relèvent de la responsabilité des unités régionales de la Police fédérale ou des polices locales, ces dernières demandent aux RCCU de leur fournir un appui technique, ce qui implique que les RCCU consacrent 90 % de leur temps à cet appui.

Faute de ressources humaines au sein des RCCU, les LCCU effectuent des enquêtes liées à des preuves numériques sans avoir les compétences nécessaires et, dans le même temps, les RCCU sont incapables de mener leurs propres enquêtes.

Le risque que les enquêtes en souffrent étant élevé, les autorités belges devraient s'attacher à y remédier en confiant à la FCCU un rôle de coordination et la mission consistant à définir un ensemble de bonnes pratiques et des formations contraignantes pour toutes les unités concernées.

Mais, pour ce faire, il faudrait que le budget de la FCCU et des RCCU soit augmenté en gardant à l'esprit que les capacités en matière de preuves numériques ne sont pas seulement nécessaires pour les incriminations spécifiquement liées à la cybercriminalité, mais aussi pour toutes les autres incriminations, y compris celles qui concernent le terrorisme et d'autres formes de criminalité organisée.

Il y a lieu de noter que l'un des points fondamentaux du nouveau plan national de sécurité 2016-2019 intitulé "*Aller ensemble à l'essentiel*" consiste à "*améliorer l'approche policière de la criminalité informatique, en tenant compte des évolutions d'internet, de l'innovation et des nouvelles technologies*". Pour ce faire, il est préconisé d'"*organiser des mesures coordonnées dans l'approche de la cybercriminalité et de la cybersécurité, et [de] renforcer l'expertise et les connaissances des services de police à ce sujet*".

Lors de la visite d'évaluation, dans les discussions avec les divers services de la police fédérale, régionale et locale, plusieurs points critiques ont été rapportés à l'équipe d'évaluation. Les plus marquants d'entre eux sont les suivants:

- pénurie d'effectifs;
- procédure de recrutement non adaptée au profil recherché;
- nombre insuffisant de formations;
- non-anticipation lors du départ de collaborateurs;
- rémunérations non adaptées (le policier classique gagne plus qu'un policier spécialiste au niveau central);
- concurrence entre les différents services (FCCU, RCCU et LCCU);
- moyens insuffisants (par exemple un seul accès internet (LENT) pour 10 enquêteurs de la section CSAM);
- montant du budget de formation nettement insuffisant.

On peut tout de même mettre en évidence que les problèmes cités ci-dessus ont été clairement identifiés par les praticiens.

Le plan national de sécurité 2016-1019 contient une mention expresse qui vise l'amélioration de l'approche de la police face à la lutte contre la cybercriminalité. De ce fait, il faudra que les autorités politiques répondent à cette priorité en dotant les services répressifs de moyens et d'effectifs adaptés pour qu'ils puissent remplir leurs missions de façon satisfaisante.

Sur le plan institutionnel, l'équipe d'évaluation reconnaît l'investissement consenti par le ministère public en faveur de la spécialisation de quelques magistrats au sein du Parquet fédéral et des parquets régionaux.

Il convient de mettre en exergue la décision de nommer le procureur général d'Anvers en tant que responsable de la coordination en matière de cybercriminalité, la centralisation auprès du Parquet fédéral des compétences en matière de cybercriminalité, en liaison avec la FCCU (circulaire 9/2009), la création d'un réseau d'expertise au sein du Collège des procureurs généraux et la nomination, dans chaque parquet régional, de magistrats de référence pour la cybercriminalité.
Au niveau judiciaire, l'équipe d'évaluation a constaté une formation insuffisante des juges, en particulier les juges d'instruction, surtout par rapport à leurs compétences d'enquête.

5 ASPECTS JURIDIQUES

5.1 Droit pénal matériel en matière de cybercriminalité

5.1.1 Convention du Conseil de l'Europe sur la cybercriminalité

Le Royaume de Belgique est partie à la "Convention de Budapest" qu'il a ratifiée par la loi du 3 août 2012 portant assentiment à la Convention sur la cybercriminalité, faite à Budapest le 23 novembre 2001. Cette loi a été publiée au Moniteur belge du 21 novembre 2012 et est entrée officiellement en vigueur le 1er décembre 2012.

Quelques réserves y sont formulées et un certain nombre de déclarations y sont faites par le gouvernement belge. Les réserves concernent essentiellement l'article 22 de la Convention de Budapest, qui prévoit une réglementation sur la juridiction que les parties à la convention doivent établir à l'égard de toute infraction pénale établie conformément à la convention. Une autre réserve concerne les infractions de piratage interne (art. 550bis, § 2, du Code pénal) et le faux en informatique (art. 210bis du Code pénal) qui font l'objet d'une interprétation plus restrictive en droit belge, étant donné qu'elles doivent avoir été commises soit avec une intention frauduleuse, soit dans le but de nuire.

5.1.2 Description de la législation nationale

A/ Décision-cadre 2005/222/JAI du Conseil et Directive 2013/40/UE relatives aux attaques contre les systèmes d'information

Au Titre IX bis du Livre II du Code pénal sur 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", figurent les incriminations de piratage et de sabotage de données et de systèmes.

1. Piratage (art. 550bis du Code pénal)
En ce qui concerne le piratage, sont visés:

a) le piratage externe (art. 550bis, § 1er, du Code pénal); b) le piratage interne (art. 550bis, § 2, du Code pénal); c) les infractions liées à des "outils de piratage" (art. 550bis, § 5, du Code pénal); d) l'incitation au piratage (art. 550bis, § 6, du Code pénal); e) le recel de données obtenues par piratage (art. 550bis, § 4, du Code pénal); f) la manipulation de données dans un système informatique (art. 550ter, § 1er, du Code pénal).

2. Sabotage de données et de systèmes (art. 550ter du Code pénal)

En ce qui concerne le sabotage, sont visées:

a) les infractions relatives à des outils de sabotage de données et de systèmes (art. 550ter, § 4, du Code pénal);

b) l'interception illégale de données informatiques (art. 259bis et 314bis du Code pénal).

Relèvent également de cette catégorie la captation punissable de données pendant leur transmission ("infractions d'écoute"), visée aux art. 259bis et 314bis du Code pénal, et la captation punissable de données avant, après ou en dehors de leur transmission (art. 550bis, §§ 1er et 2, et § 3, 1°, du Code pénal).

Les règles de droit commun en matière de responsabilité pénale de la personne morale sont d'application. En droit pénal belge, conformément à l'article 5 du Code pénal, les personnes morales ont une responsabilité pénale autonome pour leurs actes, indépendamment des éventuels comportements de la personne physique par laquelle elles agissent.

En principe, toutes les infractions entrent en ligne de compte pour la responsabilité pénale des personnes morales, y compris les infractions informatiques. Le législateur n'a pas instauré de limitations en la matière.

L'imputation matérielle d'une infraction (informatique) à la personne morale (composante objective de la qualité d'auteur) est possible, conformément à l'article 5, alinéa 1er, du Code pénal, uniquement lorsqu'un lien intrinsèque existe entre l'infraction et la personne morale, en d'autres termes lorsque l'infraction a été commise: pour la réalisation de l'objet social ou en défense des intérêts de la personne morale, ou lorsque les faits concrets démontrent qu'elle a été commise pour son compte. Ces critères sont alternatifs, ce qui n'exclut bien entendu pas que la composante matérielle de la qualité d'auteur de la personne morale soit également présente si plusieurs critères sont remplis. Ce qui précède n'implique toutefois pas que tout événement matériel comportant un lien intrinsèque avec l'objet de la personne morale, avec la défense de ses intérêts ou qui a été commis pour son compte, puisse lui être automatiquement imputé.

Comme c'est le cas pour les personnes physiques, la personne morale doit être responsable de l'infraction (informatique) (composante subjective de la qualité d'auteur). En d'autres termes, l'infraction doit pouvoir lui être reprochée. Cela signifie que la personne morale, tout comme la personne physique, ne peut être pénalement responsable que si on retrouve chez elle tant la composante matérielle que la composante morale de la qualité d'auteur. C'est la logique pénale qui est ainsi suivie: c'est celui qui commet l'infraction qui est puni. Même si la faute de la personne morale est étroitement liée à celle de la personne physique, il n'en demeure pas moins qu'une faute pénale pertinente doit se retrouver chez les deux personnes. Le tribunal devra également constater la faute chez la personne morale. La jurisprudence de la Cour de cassation confirme que les personnes morales disposent d'une volonté propre qui peut être source d'infractions, bien qu'elles agissent *de facto* par l'intermédiaire d'individus. Pour l'imputation morale d'une infraction à une personne morale (imputabilité), cette volonté doit également être démontrée; cette volonté ne peut être simplement déduite de la volonté de la personne physique.

L'article 7bis du Code pénal a instauré les peines applicables aux infractions commises par les personnes morales. Il a été ainsi opté pour l'amende comme peine principale. L'article 41bis du Code pénal prévoit un mécanisme de conversion des peines privatives de liberté pour les personnes physiques en amendes pour les personnes morales. L'art. 7bis du Code pénal prévoit en outre un certain nombre de peines accessoires spécifiques.

Le droit belge ne comprend pas de critères comme l'incidence économique, politique ou sociale importante, le nombre de systèmes touchés ou la hauteur du préjudice. Par contre, l'article 550ter, § 3, du Code pénal comprend le critère de celui qui "empêche, totalement ou partiellement, le fonctionnement correct du système informatique concerné ou de tout autre système informatique" comme circonstance aggravante.

Le droit belge ne connaît pas de "cas légers" dans le Code pénal. Il appartient à l'instance poursuivante de juger si une certaine infraction doit faire l'objet de poursuites. En effet, le ministère public dispose d'une décision d'opportunité de poursuivre ou non et/ou peut également proposer des modalités de règlement alternatives (médiation pénale, transaction, probation prétorienne, etc.).

Outre les actes punissables de cybercriminalité déjà mentionnés, il existe plusieurs actes de cybercriminalité pour lesquels des incriminations sont prévues et qui ne relèvent d'aucune des trois catégories prévues pour l'évaluation GENVAL. Il convient de mentionner à ce sujet les incriminations prévues dans la loi relative aux communications électroniques.

Il existe en effet plusieurs infractions *informatiques dans la législation particulière, comme le prévoit la* loi du 13 juin 2005 relative aux communications électroniques, qui donnent lieu à un vaste arsenal de dispositions pénales, dont un certain nombre se répartissent moins facilement dans cette classification, alors que la distinction avec les dispositions pénales qui figurent au Livre II du Code pénal ne semble par ailleurs pas toujours nette (art. 145, § 3*bis*, 124, 1° et 4° de la loi du 13 juin 2005 relative aux communications électroniques[12]). Il y a en outre le Code de droit économique, Livre XII, Droit de l'économie électronique (anciennement la loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information; art. 21 et 26 de la loi du 11 mars 2003).

Le plan Justice du ministre de la Justice exprime, en matière de cybercriminalité et de criminalité par le biais de l'internet, la volonté de mettre en œuvre les adaptations les plus urgentes.

Un projet de loi visant à augmenter les peines aux articles 314bi*s* et 550bis du Code pénal a été soumis à la cellule stratégique du ministre de la Justice. Ce projet vise à transposer intégralement la directive 2013/40/EU.

[12] M.B. 20 juin 2005.

Le droit belge est en grande partie conforme aux dispositions de cette directive. Un tableau de concordance a déjà été transmis à la Commission européenne. Un projet de loi visant à augmenter les peines aux articles 314bis et 550bis du Code pénal a été soumis à la cellule stratégique du ministre de la Justice. Ce sont les seules modifications qui sont nécessaires en vue d'une conformité entière avec la directive.

Le récent article 371/1 du Code pénal sur le voyeurisme incrimine l'espionnage direct ou en recourant à un moyen technique ou autre d'une personne dénudée ou se livrant à un acte sexuel explicite, ainsi que la diffusion de l'enregistrement visuel ou audio d'une personne dénudée ou se livrant à une activité sexuelle explicite, sans son accord ou à son insu, même si cette personne a consenti à sa réalisation.

B/ Directive 2011/93/UE du Parlement Européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil

La Belgique a transposé dans sa législation nationale la quasi-totalité de la directive 2011/93/UE. Quelques petites modifications ponctuelles étaient encore nécessaires. À cet effet, le Conseil des ministres a approuvé le 16 octobre 2015, sur la proposition du ministre de la Justice Koen Geens, un avant-projet de loi complétant la mise en œuvre des obligations européennes en matière d'exploitation sexuelle des enfants, de pédopornographie, de traite des êtres humains et d'aide à l'entrée, au transit et au séjour irréguliers.

L'avant-projet de loi poursuit trois objectifs:

- la poursuite de la mise en conformité de la législation belge avec la directive européenne 2011/36/UE concernant la prévention de la traite des êtres humains et la lutte contre ce phénomène ainsi que la protection des victimes;
- des modifications ponctuelles relatives au droit pénal et à la procédure pénale afin de compléter la conformité aux exigences de la directive européenne 2011/93/UE relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants ainsi que la pédopornographie;
- la poursuite de la mise en conformité de la législation belge avec la directive 2002/90/CE définissant l'aide à l'entrée, au transit et au séjour irréguliers et le renforcement du cadre pénal pour la répression de l'aide à l'entrée, au transit et au séjour irréguliers.

Dans ce cadre, une solution est également proposée en vue de la suppression de sites internet, afin de répondre aux exigences de l'article 25, paragraphe 1, de la directive selon lequel cette suppression doit être rapide.

À présent, l'avant-projet de loi est soumis pour avis au Conseil d'État et il sera ensuite soumis au débat parlementaire.

Les incriminations classiques en matière de délinquance sexuelle sont avant tout appliquées lorsque des technologies de l'information et de la communication sont l'objet d'abus pour adopter un comportement sexuel pénalement punissable envers des mineurs.

Il s'agit par conséquent des incriminations d'attentat à la pudeur et de viol (art. 372-378bis du Code pénal), d'incitation à la débauche de mineurs, corruption de la jeunesse et prostitution (art. 379-382quater du Code pénal) et de la détention ou fabrication de pédopornographie (art. 383bis du Code pénal).

Il convient de mentionner spécifiquement à cet égard deux lois qui s'inscrivent dans un mouvement de modernisation du Code pénal en matière de criminalité sexuelle à l'égard d'enfants et de jeunes, par le biais de l'internet ou d'autres technologies de l'information et de la communication.

La loi du 30 novembre 2011 modifiant la législation en ce qui concerne l'amélioration de l'approche des abus sexuels et des faits de pédophilie dans une relation d'autorité (art. 7 et 12 de la loi du 30 novembre 2011) a introduit une incrimination élargie de la pédopornographie, qui s'applique depuis le 30 janvier 2012. Outre la "détention punissable", l'"accès punissable à" est lui aussi devenu punissable. Quiconque accède en connaissance de cause, par le biais d'un système informatique ou de tout autre moyen technologique, à de la pédopornographie risque, à la suite de cette loi, les mêmes peines qu'une personne détenant du matériel pédopornographique. Cela s'inscrit dans le cadre de l'application de la Convention de Lanzarote concernant la protection des enfants contre l'exploitation sexuelle.

Avec le même objectif et en exécution de la Convention de Lanzarote du Conseil de l'Europe et de la directive UE relative à la lutte contre les abus sexuels (directive 2011/92/UE du Parlement européen et du Conseil du 13 décembre 2011, JO L du 17 décembre 2011), la loi du 10 avril 2014 relative à la protection des mineurs contre la sollicitation à des fins de perpétration d'infractions à caractère sexuel a inséré, dans le chapitre du Code pénal relatif aux infractions "attentat à la pudeur" et "viol", une nouvelle circonstance aggravante pour l'infraction "grooming" (en ligne) (art. 377ter et 377quater du Code pénal). Cette même loi a également introduit la nouvelle incrimination de cyberprédation (art. 433bis/I du Code pénal).

Les nouvelles dispositions pénales spécifiques prouvent sans conteste leur utilité dans la pratique vis-à-vis des incriminations classiques dans le cadre de la lutte contre l'abus d'enfants par le biais de l'internet ou d'autres technologies de l'information ou de la communication, mais contribuent par ailleurs malheureusement à rendre de plus en plus confus le droit pénal sexuel belge en général et le droit pénal sexuel visant à protéger les mineurs en particulier.

C/ Fraude en ligne aux cartes de paiement

Les citoyens et les sociétés privées signalent presque toujours les fraudes aux cartes de paiement à la police (locale) parce que les banques exigent une copie du PV/de la déclaration à la police pour rembourser le montant de la fraude.

La FCCU de la Police fédérale participe au groupe de travail "Internet banking security" qui se penche sur les vulnérabilités et menaces de la fraude à la banque en ligne. Dans le cadre de l'optimalisation de la Police fédérale, il a été décidé qu'il n'y a pas de suivi national concernant les autres formes de fraude à la carte de paiement; ces dossiers sont gérés par les services de la Police fédérale des arrondissements, qui ont également de bons contacts avec l'industrie, mais plutôt au cas par cas.

Les infractions relatives à la fraude en ligne aux cartes de paiement incluent:
- le faux et l'usage de faux en informatique (art. 210bis du Code pénal)
a) faux en informatique (art. 210bis, § 1er du Code pénal);
b) usage de fausses données informatiques (art. 210bis, § 2 du Code pénal)
- la fraude informatique (art. 504quater du Code pénal)
- le vol d'identité (pas d'incrimination spécifique)
Il convient de signaler à cet égard qu'il n'existe pas d'incrimination spécifique en Belgique pour le vol d'identité, mais des poursuites peuvent être engagées sur la base d'autres dispositions pénales. Il est qualifié notamment de port de faux nom (art. 231 du Code pénal) et de faux en écritures.

D/ Autres phénomènes de cybercriminalité

La législation belge applicable en matière de cybercriminalité se contente de trois grandes catégories d'infractions:

- 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 (sabotage, piratage, etc.).

Selon l'équipe d'évaluation, l'arsenal législatif belge est relativement adéquat en ce qu'il permet d'encadrer la majorité des comportements nuisibles commis sur et à l'aide de l'internet.

5.2 Questions de procédure

5.2.1 Techniques d'investigation

Toutes les techniques d'investigation mentionnées dans le questionnaire GENVAL sont autorisées par la loi belge.

- **la perquisition et la saisie de systèmes d'information/de données informatiques**

En droit belge, il y a avant tout la possibilité de saisie de supports matériels de données conformément à l'article 35 et suivants du Code d'instruction criminelle (CIC). Il y a en outre la possibilité de saisie de données conformément aux art. 39bis et 89 du CIC. Il existe également une possibilité de recherche sur réseau conformément à l'article 88ter du CIC.

- **l'interception/la collecte en temps réel de données relatives au trafic/au contenu**

Le droit belge permet la captation de données pendant leur transmission ou l'"écoute informatique", comme le prévoit l'art. 90ter du CIC.

- **la conservation de données informatiques**

Conformément à l'art. 88bis du CIC, il est possible de procéder à un enregistrement des communications sur l'internet ou de l'utilisation de l'internet.

Les règles de droit en matière de conservation des données ont été transposées en droit belge et figuraient à l'article 126 de la loi relative aux communications électroniques. Cette réglementation a toutefois été annulée par l'arrêt n° 84/2015 de la Cour constitutionnelle du 11 juin 2015. La Cour constitutionnelle a ainsi suivi l'évaluation de l'arrêt de la Cour de justice du 8 avril 2014 (CJUE, 8 avril 2014, C-293/12 et C-594/12) donnant lieu à l'annulation de la directive relative à la conservation des données.

Une nouvelle réglementation légale de droit interne est actuellement en cours d'élaboration en la matière.

- **l'injonction de produire des données stockées relatives au trafic/au contenu**

Il convient d'établir une distinction entre l'enregistrement et la conservation des données par le fournisseur de télécommunications, d'une part, et la demande de ces données dans le cadre d'une enquête pénale par l'autorité judiciaire compétente, d'autre part.

Sur la base de l'article 88bis du CIC, les données de localisation et de trafic peuvent être valablement demandées par l'autorité compétente.

Conformément à l'article 126, § 2 in fine de la loi du 13 juin 2005 relative aux communications électroniques, les données collectées dans le cadre de la conservation des données devaient être transmises sur simple demande. Il n'y a actuellement aucune obligation de communication, eu égard à l'annulation de la disposition "conservation des données".

- **l'injonction de communiquer des données concernant l'utilisateur**

L'identification d'abonnés/utilisateurs et de services/moyens de communication (art. 46bis et 56, § 1er, du Code d'instruction criminelle).

Il s'agit de dispositions assez dépassées car initialement destinées aux repérages et écoutes téléphoniques; une réforme liée à la transposition de la directive "conservation des données" (2006/24/CE) a été censurée par un arrêt de la Cour constitutionnelle du 11 juin 2015.

Les services de renseignement et de sécurité belges (la Sûreté de l'État et le Service général du renseignement et de la sécurité) ont, depuis la loi du 4 février 2010[13] (modifiant la loi organique des services de renseignement et de sécurité du 30 novembre 1998), la compétence pour recourir aux méthodes ordinaires (art. 14 à 18), spécifiques et exceptionnelles (art. 18/1 à 18/18) pour recueillir des données et réaliser les objectifs qui leur sont assignés.

Ces articles prévoient notamment les techniques spéciales d'investigation suivantes: la possibilité d'une identification de l'abonné ou de l'utilisateur d'un service de communications électroniques, l'écoute de télécommunications et le piratage informatique.

[13] M.B. du 4 février 2010.

Les méthodes particulières de recherche auxquelles peuvent recourir les autorités judiciaires compétentes sont énumérées aux articles 47ter et suivants du CIC. Il s'agit des méthodes d'observation, d'infiltration et de recours à des indicateurs.

Dans les grands dossiers en matière de cybercriminalité, certainement ceux dont le monde bancaire est la victime, le gain d'argent pour les cybercriminels est un élément très important. La Belgique a utilisé cet élément comme point de départ pour ouvrir certains dossiers. À côté de l'enquête de cybercriminalité, est également mise en place une enquête financière. A ce titre, le travail des enquêteurs en matière financière et de cybercriminalité dans le cadre d'équipes multidisciplinaires s'avère efficace.

5.2.2 Examen criminalistique et chiffrement

Les services de police, en particulier la Federal Computer Crime Unit et les Regional Computer Crime Units, réalisent des examens médico-légaux numériques, également à distance.

Le chiffrement pose un problème réel et de plus en plus présent, non seulement dans les examens criminalistiques, mais également dans tout autre type d'enquête:

- incapacité d'analyser des volumes cryptés "TrueCrypt" sans la coopération du suspect;
- utilisation de moyens de communication du type "WhatsApp" et "Telegram", principalement sur les smartphones;
- utilisation des protocoles HTTPs pour les sites les plus courants (Google, Facebook, etc.);
- dans certains cas, la clef de chiffrement n'est pas disponible auprès des fournisseurs de services (éditeurs du logiciel), mais est générée et gérée uniquement par les utilisateurs;
- l'apparition de la technologie "second proxy" mise en place par les grands fournisseurs de services, tels Facebook et Google, qui vont jusqu'à les incorporer dans leurs systèmes Android ou Chrome. Cette technologie remplace les requêtes DNS effectuées par le dispositif utilisé par l'utilisateur final en effectuant l'ensemble des requêtes à l'intérieur du tunnel encrypté HTTPS, , en ne laissant plus aucune donnée non cryptée disponible pour l'enquête.

5.2.3 Preuves électroniques (E-evidence)

Le droit belge n'a pas de dispositions spécifiques concernant la preuve électronique. En général, des copies des données utilisées comme preuve sont réalisées sur DVD ou disque dur. À cet égard, on peut renvoyer à la circulaire confidentielle COL 16/2004 du Collège des procureurs généraux, à laquelle a été jointe une annexe technique portant des directives relatives aux examens médico-légaux et au traitement d'informations numériques.

La preuve en matière pénale est régie par le Code d'instruction criminelle et les principes du droit de la procédure pénale. En règle générale, l'administration de la preuve est libre (principe de la liberté de la preuve). Il n'y a pas de conditions d'admissibilité particulières pour les preuves électroniques.

L'art. 32 du Titre préliminaire au Code d'instruction criminelle prévoit les critères qui sont appliqués concernant l'admissibilité de la preuve: "*La nullité d'un élément de preuve obtenu irrégulièrement n'est décidée que si:*
- le respect des conditions formelles concernées est prescrit à peine de nullité, ou;
- l'irrégularité commise a entaché la fiabilité de la preuve, ou;
- l'usage de la preuve est contraire au droit à un procès équitable".

L'art. 13 de la loi du 9 décembre 2004 sur l'entraide judiciaire internationale en matière pénale[14] règle la situation concernant la preuve à l'étranger: "*Ne peuvent être utilisés dans le cadre d'une procédure menée en Belgique, les éléments de preuve: 1° recueillis irrégulièrement à l'étranger, lorsque l'irrégularité: - découle, selon le droit de l'État dans lequel l'élément de preuve a été recueilli, de la violation d'une règle de forme prescrite à peine de nullité;; - entache la fiabilité de la preuve;; 2° ou dont l'utilisation viole le droit à un procès équitable."*

[14] M.B. 24 décembre 2004.

5.3 Protection des droits de l'homme/libertés fondamentales

La Constitution belge garantit les libertés fondamentales inspirées notamment de la Déclaration des droits de l'homme et du citoyen. Il n'existe pas de législation spécifique concernant ces principes pour l'internet.

La montée en puissance des nouveaux médias et des données informatisées est prise en considération par la Commission pour le protection de la vie privée qui, parallèlement à des actions de sensibilisation, dispose d'outils coercitifs et répressifs. Les publications, dont le rapport annuel, sont disponibles sur le site internet de la commission[15].

Outre cela, la recherche, la poursuite et le jugement de faits de criminalité informatique représentent, tout comme l'utilisation des technologies de l'information et de la communication (TIC) dans les procédures pénales et l'établissement de positions d'information, une intrusion significative dans les droits fondamentaux. Dans le système juridique belge, nous en sommes parfaitement conscients. Les principes suivants sont respectés autant que possible dans le droit belge:

- Toute restriction au droit à la vie privée doit être prévue par la loi et doit être proportionnée, légitime et nécessaire dans une société démocratique.

- L'utilisation des TIC dans les procédures pénales et la création de positions d'information doivent respecter le droit à la protection des données. Les objectifs de la prévention de la criminalité et l'enquête pénale sont équilibrés par rapport à l'empiètement des droits fondamentaux à la protection des données.

15 https://www.privacycommission.be/fr.

- Le principe de limitation de la finalité est respecté, plus particulièrement lors d'une transmission de données électroniques à caractère personnel aux autorités chargées de l'application de la loi. Le principe de limitation de la finalité signifie que les données à caractère personnel ne peuvent être recueillies que pour une finalité explicite, déterminée et légitime, excluant un traitement ultérieur incompatible avec les finalités pour lesquelles les données ont été collectées.

- Il ne peut être dérogé à la limitation de la finalité que dans les cas exceptionnels, prévus par la loi, où le transfert des données aux autorités chargées de l'application de la loi est nécessaire pour la prévention, l'enquête ou les poursuites d'un crime grave et respecte le principe de proportionnalité.

- Le cadre juridique doit assurer, de façon plus générale et dans la mesure du possible, que des moyens et des seuils adéquats pour l'accès et la divulgation des données stockées sont établis et contrôlés par une autorité indépendante. Si une obligation de tenir à jour, de conserver et d'envoyer des données informatiques incombe à une entreprise publique et/ou privée, celle-ci doit respecter le droit à la protection des données.

- L'utilisation des TIC dans les procédures pénales ne peut porter atteinte aux droits de la défense, notamment le droit à une audience publique, le droit au contre-interrogatoire et à la confrontation, le droit d'accès au dossier et le droit à l'assistance d'experts spécialisés dans le domaine de la preuve électronique, afin d'assurer le principe de l'égalité des armes.

5.4 Compétence

5.4.1 Principes appliqués pour enquêter sur la cybercriminalité

Lorsqu'un des éléments constitutifs d'une qualification d'infraction peut être localisé sur le territoire de la Belgique, les autorités belges sont compétentes.

La réponse comporte tout de même deux volets, à savoir si les infractions informatiques sont commises en partie ou totalement sur le territoire belge.

a) Pour les infractions informatiques qui sont commises **en partie** en dehors du territoire du Royaume, nous pouvons évoquer le **principe de territorialité**. L'article 3 du Code pénal dispose que: "L'infraction commise sur le territoire du royaume, par des Belges ou par des étrangers, est punie conformément aux dispositions des lois belges." L'art. 3 du Code pénal respecte par conséquent le principe de territorialité en ce qui concerne le champ d'application du droit pénal positif: la loi pénale s'applique uniquement au territoire national, sauf exceptions découlant de dispositions du droit interne ou de conventions internationales.

En principe, la Belgique est par conséquent compétente si l'infraction a été entièrement commise sur le territoire mais également si elle y a été commise en partie. Le principe de territorialité comme critère de pouvoir juridictionnel a en effet évolué d'une compétence uniterritoriale à une compétence en partie territoriale ou un concept de territorialité élargie.

En Belgique, nous appliquons la théorie de l'ubiquité objective aux comportements multiterritoriaux. Si une infraction se produit sur le territoire de différents États (infraction multiterritoriale), la Belgique est compétente lorsqu'un des éléments constitutifs (objectifs) (parties de l'élément matériel) d'une qualification d'infraction belge peut être localisé en Belgique. La localisation sur le territoire ne peut se faire que par le biais de la localisation d'éléments qui sont constitutifs de l'infraction. Ainsi, la suite de l'infraction conduira uniquement à une juridiction territoriale si cette suite est un élément constitutif de l'infraction (la suite *constitutive*). Cela dépend bien entendu de l'article de loi spécifique.

La jurisprudence belge estime en outre que les tribunaux belges exercent également leur compétence territoriale lorsqu'ils jugent qu'une infraction commise à l'étranger forme un tout indivisible avec une infraction localisée en Belgique. Ainsi, les juges belges s'estiment notamment compétents pour des participants étrangers à l'infraction belge ou des comportements punissables étrangers qui forment un tout indivisible avec les actes punissables posés en Belgique (infractions continues et, ce qui est moins évident, infractions continuées). Ils s'estiment par ailleurs compétents territorialement lorsqu'une partie ou un aspect indissociable de l'infraction se manifeste sur le territoire belge. Ils entendent par là également les conséquences qui ne se manifestent qu'une fois l'infraction commise, mais qui forment néanmoins avec l'infraction un tout indivisible. Cela entraîne parfois des applications extraterritoriales "déguisées" de la loi pénale belge. Sous le couvert de l'application territoriale de la loi pénale, la loi pénale belge s'applique à des faits commis à l'étranger. Son champ d'application *ratione loci* dépasse donc le territoire belge. On crée ainsi une construction juridique où les faits sont *censés* avoir été commis en Belgique. La combinaison par la jurisprudence belge de la théorie de l'ubiquité objective à la théorie de l'indivisibilité peut entraîner une application de fait de la théorie des effets. À ce niveau, le juge pénal prend non seulement en considération les effets constitutifs de l'infraction, mais également les autres effets éliminés.

b) Pour la criminalité informatique qui est **entièrement** commise en dehors du territoire de l'État membre, les règles de droit commun de l'applicabilité de la loi pénale belge s'appliquent aux faits commis à l'étranger. L'article 4 du Code pénal dispose que: "L'infraction commise hors du territoire du royaume, par des Belges ou par des étrangers, n'est punie, en Belgique, que dans les cas déterminés par la loi".

Les exceptions sont indiquées principalement aux articles 6 à 14 du titre préliminaire du Code de procédure pénale. Ces exceptions se fondent sur plusieurs principes.

Le **principe de la personnalité ou de la nationalité active**, fondé sur la nationalité de l'auteur, d'où l'application de la loi pénale belge sur les Belges qui se rendent coupables à l'étranger de crimes ou de délits (art. 7 et 9 du titre préliminaire du Code de procédure pénale). Ce principe est lié au principe selon lequel les États n'extradent généralement pas leurs propres ressortissants.

Le **principe de protection ou de la nationalité passive**, fondé sur la nationalité de la victime, d'où l'application de la loi pénale belge sur les étrangers qui ont commis à l'étranger certains crimes ou délits contre un ressortissant belge. Il n'a été instauré que par la loi du 12 juillet 1981 (art. 10, 5°, du titre préliminaire du Code de procédure pénale). Il s'appliquait auparavant uniquement aux infractions commises en temps de guerre (art. 10, 4°, du titre préliminaire du Code de procédure pénale).

Le **principe de protection de l'État**, fondé sur l'idée que l'ordre social interne est d'abord perturbé par des faits commis à l'étranger quand l'État belge est la victime directe des faits commis, d'où l'application de la loi pénale belge aux infractions contre la sûreté de l'État ou contre les valeurs monétaires belges et l'euro, commises par quiconque, belge ou étranger, en dehors de notre territoire (art. 6, 1° et 2° et 10, 1° et 2° du titre préliminaire du Code de procédure pénale). Le principe de protection de l'État est également lié au fait que de telles infractions ne sont pas toujours punissables selon la législation du *locus delicti*.

Le **principe d'universalité**, fondé sur la nature de l'infraction et les intérêts de la communauté internationale. La loi du 16 juillet 1993 avait attribué une large portée à ce principe en ce qui concerne les violations graves du droit humanitaire international. Sous la pression américaine, cette loi a été abrogée par la loi du 5 août 2003. Le principe d'universalité est actuellement principalement en vigueur pour les infractions contre les moyens de paiement d'un pays étranger (art. 6, 3° et 10, 3° du titre préliminaire du Code de procédure pénale) et à la suite des lois du 13 avril 1995 et du 28 novembre 2000 concernant les infractions sexuelles (art. 10*ter* du titre préliminaire du Code de procédure pénale).

5.4.2 Règles en cas de conflits de compétence et d'aiguillage à Eurojust

Comme indiqué à la question 1, la compétence territoriale matérielle ou la détermination du *locus delicti* dans le cyberespace s'effectuent essentiellement au moyen de la théorie de l'ubiquité objective et de la théorie de l'indivisibilité, sur la base de l'article 3 du Code pénal.

En raison de ce concept de territorialité élargie, il peut en effet arriver que différents États et la Belgique soient également compétents pour les mêmes faits. Si différents États appliquent cette approche, cela peut générer des difficultés. Il est en effet possible que l'on travaille simultanément sur les mêmes suspects ou groupes d'auteurs ou que des faits fassent l'objet de poursuites, faits qui, aux yeux d'un autre État concerné, ne sont pas punissables.

En cas de litige portant sur la juridiction, lorsque deux ou plusieurs États membres peuvent ouvrir une enquête ou entamer des poursuites à l'encontre du même auteur, une concertation avec les États membres concernés a lieu, au besoin par l'intermédiaire d'Eurojust, afin de passer des accords pratiques.

En outre, en Belgique, le principe général du droit "ne bis in idem" s'applique également à la cybercriminalité.

Des dossiers ont déjà été soumis à Eurojust pour des dispositions relatives à la décision-cadre 2009/948/JAI du Conseil du 30 novembre 2009 relative à la prévention et au règlement des conflits en matière d'exercice de la compétence dans le cadre de procédures pénales concernant des affaires de cybercriminalité et les expériences en la matière se sont avérées positives. Dans certains cas, cela a abouti à la création d'une ECE (équipe commune d'enquête).

5.4.3 Compétence pour les actes de cybercriminalité commis dans le "nuage"

La recherche extraterritoriale est permise lorsqu'il s'avère que ces données ne se trouvent pas sur le territoire. Les données peuvent seulement être copiées (et non bloquées).
Une information doit être transmise au ministère de la Justice qui informe les autorités compétentes de l'État concerné.

5.4.4 Perception de la Belgique à l'égard du cadre juridique pour lutter contre la cybercriminalité

Les instruments d'entraide judiciaire internationale sont insuffisants face à l'environnement de preuve volatile de l'internet, lequel requiert une réaction rapide et des instruments souples.

5.5 Conclusions

Le cadre législatif belge est relativement adéquat à la lutte contre la cybercriminalité. L'équipe d'évaluation salue les efforts entrepris par la Belgique en vue d'élaborer une loi relative à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant l'internet, les communications électriques et les télécommunications.

L'équipe d'évaluation salue également la persévérance de la justice belge dans la controverse avec l'entreprise américaine YAHOO. Le tribunal belge peut s'adresser directement à YAHOO pour obtenir des données d'identification dans le cadre d'une enquête.

À l'époque de l'évaluation, le gouvernement était saisi de la question de la loi sur la conservation des données, que la Cour constitutionnelle avait déclarée inconstitutionnelle (décision du 11 juin 2015). Après la visite d'évaluation, la loi a été promulguée le 18 juillet (loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des télécommunications).
Il faut souligner la nécessité d'une harmonisation européenne dans ce domaine, comme dans celui des devoirs de collaboration directe sans entraide judiciaire auxquels sont soumis les fournisseurs de services qui permettent l'accès sur le territoire européen (jurisprudence Yahoo).

Après la visite d'évaluation, les autorités nationales ont informé l'équipe des évaluateurs que la législation belge sur les méthodes particulières avait été mise à jour par la "*loi du 25 décembre 2016 portant des modifications diverses au Code d'instruction criminelle et au code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales*".

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

- clarification et amélioration du régime pour la recherche non secrète dans un système informatique;
- mise en œuvre de la convention sur la cybercriminalité par la création d'une procédure de gel des données;
- extension du contrôle visuel discret;
- création d'une mesure spécifique pour les interactions ou infiltrations ayant exclusivement lieu sur l'internet;
- en matière d'interception des télécommunications: fusion de la recherche secrète dans un système informatique avec l'interception des télécommunications et extension de la liste des infractions pour lesquelles la mesure est possible;
- base légale pour une banque de données des empreintes vocales qui apparaissent dans les interceptions des télécommunications.

Une loi de réparation a été adoptée le 29 mai 2016 (*loi relative à la collecte et à la conservation des données dans le secteur des communications électroniques*). Plusieurs recours en annulation ont été introduits devant la Cour constitutionnelle contre cette loi depuis l'arrêt de la Cour de justice de l'Union européenne du 21 décembre 2016.

La "*loi du 31 mai 2016 complétant la mise en œuvre des obligations européennes en matière d'exploitation sexuelle des enfants, de pédopornographie, de traite des êtres humains et d'aide à l'entrée, au transit et au séjour irréguliers"* complète et finalise la transposition de la directive 2011/93/UE (abus sexuels et exploitation sexuelle des enfants), de la directive 2011/36/UE (traite des êtres humains) et des instruments 2002/90/UE et 2002/946/UE (aide à l'entrée, au transit et au séjour irréguliers).

6 ASPECTS OPÉRATIONNELS

6.1 Cyberattaques

6.1.1 Nature des cyberattaques

Nombre d'affaires enregistrées de Cyberattaques					
Infraction	Articles du Code pénal	Nombre de faits enregistrés			
		2013	2014	2015	TRIM 3 2016
Hacking	art. 550 bis CP	1.745	2.054	2.159	1.682
Sabotage	art. 550 ter CP	1.186	431	423	349
Télécommunication / interception	art. 259 bis et art. 314 bis CP	88	84	83	49
Total		**3.019**	**2.569**	**2.665**	**2.080**
Source: Base de données de la Police arrêtée au 20/01/2017					

On remarque depuis plusieurs années une augmentation des faits de cyberattaques. En 2012, et moins clairement en 2013, nous observons un pic atypique dans les chiffres – surtout démontré par le nombre de faits de sabotage - à la suite de la vague du virus « *police ransomware* ».

6.1.2 Mécanisme de réaction aux cyberattaques

Il n'y a pas d'obligation légale mais un centre (Federal cyber emergency team) a été mis en place par l'État pour centraliser les informations et assister les entreprises (https://www.cert.be/fr).

Le Conseil des Ministres a approuvé, le 28 avril 2017, le Cyber plan national d'urgence, rédigé par le CCB, en collaboration avec tous les acteurs concernés (FCCU/CCU/CERT/SGRS, etc.). Ce plan contient une procédure de gestion des cyberincidents nationaux et des cybercrises, avec une définition claire des processus à respecter et des rôles et responsabilités de chaque acteur.

Pour les cyberattaques en dehors de l'Union, la Belgique a recours aux instruments d'entraide judiciaire dans la mesure où cela est indispensable. Il est également fait recours à un échange direct d'informations dans les limites de la législation nationale et de la législation étrangère ainsi qu'à l'échange d'informations entre polices.

6.2 Actions contre la pédopornographie et les abus sexuels en ligne

6.2.1 Banques de données identifiant les victimes et mesures destinées à éviter une revictimisation

La Police fédérale judiciaire est connectée avec la base de données ICSE (International Child Sexual Exploitation) d'Interpol. L'accès est géré par la section "pornographie enfantine" de la Direction de la lutte contre la criminalité grave et organisée (DJSOC).

En attendant une procédure définitive déterminée par la justice, la DJSOC gère les dénonciations. Pour les URL contenant CAM/CSAM/CSEM hébergés à l'étranger, un rapport est rédigé et envoyé aux pays concernés via SIENA (Europol) ou le canal Interpol.

Pour les URL (Uniform Resource Locator = adresse site web) hébergés sur le territoire belge, un procès-verbal est rédigé afin d'obtenir l'accord d'un magistrat pour clôturer l'URL.

6.2.2 Mesures de lutte contre l'exploitation et les abus sexuels en ligne, le sextage et la cyberintimidation

Des campagnes, affiches et dépliants pour expliquer les dangers aux enfants sont distribués chaque année à l'initiative de Child Focus.

Une réflexion au niveau des Communautés et Régions (en charge de l'éducation, qui n'est pas une compétence fédérale) sur l'insertion de la sensibilisation dans les programmes scolaires.

Le site de Child Focus www.clicksafe.be informe les enfants, les adolescents, les parents et les professionnels sur un usage sécurisé et responsable de l'internet. Ils peuvent trouver des informations sur le sujet, une ligne d'aide en cas de problème, des informations sur des formations et des liens vers d'autres sites intéressants. Il existe des formations "Clicksafe" proposées par Child Focus aux professionnels travaillant avec les enfants et les jeunes afin d'aider à favoriser le dialogue à propos d'un "internet sécurisé et responsable".

6.2.3 Prévention du tourisme sexuel, des spectacles pornographiques impliquant la participation d'enfants et autres

Certaines campagnes de prévention avec affiches ont eu lieu dans les aéroports et agences de voyages pour attirer l'attention des voyageurs et de la police de première ligne en décrivant le profil habituel d'un touriste sexuel.

L'ONG ECPAT (End Child Prostitution, Child Pornography and Trafficking of Children for sexual purposes) a coordonné ces campagnes. Un groupe national composé de la Police, des Affaires étrangères, de la Défense, de la Justice (Service de la politique criminelle), de la Fédération de l'industrie du tourisme, de la Fédération royale belge des transporteurs et des prestataires de services logistiques, de Plan Belgique, de Child Focus, de la Fondation Samilia et d'ECPAT Belgique a été mis sur pied. Ce groupe STOP, qui a fêté ses 10 ans, porte une attention particulière à l'influence du secteur touristique, des jeunes eux-mêmes, de l'appareil judiciaire et des autorités.

Le 6 novembre 2014, la campagne de sensibilisation "Je dis STOP" initiée par le groupe STOP, a été lancée. Dans le cadre de cette 3me campagne de sensibilisation, un site internet a été créé (www.jedisstop.be) et une brochure a été publiée. L'objectif de cette campagne est de sensibiliser à nouveau le grand public aux enfants victimes d'abus sexuels et d'informer les gens que, s'ils sont confrontés à une situation suspecte, ils peuvent aussi aider les autorités en la signalant via le site www.jedisstop.be et en remplissant le formulaire spécifique reprenant les principales informations nécessaires au lancement d'une enquête. La police belge transmet alors l'information aux collègues du pays concerné ainsi qu'à Europol et Interpol, si cela s'avère nécessaire. Quelle que soit la nationalité du signalant ou de l'auteur supposé, il est également possible d'effectuer un signalement via la nouvelle plateforme européenne en ligne www.reportchildsextourism.eu qui reprend toutes les lignes nationales de signalement en Europe.

En ce qui concerne les mesures de prévention, l'organisation Child Focus (ONG) assure les campagnes de sensibilisation et, notamment, la distribution de dépliants. Différents outils de prévention ont été développés:

- spot de prévention à propos du "sexting"[16]: à destination des jeunes entre 13 et 16 ans, qui les encourage à réfléchir aux conséquences de leur comportement sur l'internet;
- test individuel "es-tu hot sur Internet?"[17]: quiz pour les jeunes (12-17 ans) à propos des relations, des sentiments et de la sexualité;
- l'application en ligne "Qui est-ce?"[18]: application pour les jeunes (11-16 ans) à propos des discussions et rencontres avec de nouvelles personnes sur l'internet. Les jeunes peuvent y apprendre ce qui peut arriver sur le net et comment ils peuvent discuter en toute sécurité et reconnaître les interlocuteurs suspects;

[16] https://www.youtube.com/watch?v=LkJ5qcuebVA&list=UUeLTgN3i44Fcr6rERaN03fg.
[17] http://www.childfocus.be/clicksafe/clicksafetest/selftest.html.
[18] http://www.childfocus.be/clicksafe/chat/index.html.

- Appli Master F.I.N.D.[19]: application, jeux en ligne pour les jeunes à propos des médias et de la vie privée. En jouant, ils expérimentent à quel point il est facile de découvrir l'identité et les détails intimes d'une personne qui en dit trop sur elle-même;
- Point de contact "Charlie"[20]: spots pour les jeunes (10-16 ans) pour promouvoir le point de contact de Child Focus pour un usage sécurisé et responsable de l'internet et les conscientiser à propos des différentes problématiques (grooming, sexting, etc.);
- irrespect[21]: développé pour les enseignants qui travaillent avec des jeunes entre 10 et 14 ans. Il s'agit de 10 leçons avec des vidéos animées abordant le thème de la vie privée sur l'internet;
- la campagne "Surf Safe"[22] a été lancée en août 2015 afin de promouvoir le point de contact chez les plus jeunes;
- le rapport annuel à l'intention des jeunes[23] entre 12 et 18 ans a été produit en 2015. Celui-ci explique le travail de Child Focus de façon résumée et concrète.

Pour la Communauté flamande: Maintenantjenparle (http://kindinnood.be/nupraatikerover). Si un enfant a des questions au sujet d'un abus sexuel (Que faire si quelqu'un a des gestes déplacés envers toi? Quelqu'un t'oblige à faire des choses que tu ne veux pas? Tu connais quelqu'un qui est dans ce cas?), il peut chatter anonymement avec un collaborateur spécialisé de Vertrouwenscentra Kindermishandeling à Bruxelles.

Pour la Fédération Wallonie-Bruxelles: maintentenantjenparle est géré par Child Focus.

[19] http://www.childfocus.be/clicksafe/F.I.N.D/.
[20] https://www.youtube.com/watch?v=8B859LFJXUA.
[21] http://www.childfocus.be/sites/default/files/irespect_0.pdf.
[22] http://www.childfocus.be/fr/nouvelle/surf-safe-avec-child-focus.
[23] http://www.childfocus.be/sites/default/files/rapport_annuel_jeunes_2014.pdf.

Le site www.ecops.be, qui permettait aux citoyens de porter à la connaissance des autorités (Police fédérale) tout fait de criminalité en lien avec l'utilisation de l'internet (pédopornographie, mais également escroqueries, pratiques commerciales illégales, etc.), a été limité, en juillet 2015 à la dénonciation des images pédopornographiques, en raison de l'insuffisance de ressources pour traiter les messages envoyés par les citoyens. La page d'accueil a cependant été maintenue et mentionne des liens vers l'organisation Child Focus et d'autres autorités. Cette fonctionnalité permet à la fois de continuer à informer et permet également de dénoncer les sites suspects.

6.2.4 Acteurs de la lutte contre les sites contenant ou diffusant de la pédopornographie et mesures prises

Grâce à l'article 39bis, §3 du CIC, la Belgique peut bloquer des sites web. Pour des sites hébergés en Belgique, le problème ne se pose pas puisque la police peut faire une perquisition et confisquer les données. Sachant s'il est impossible de "saisir" physiquement des données numériques, la police peut copier ces données et les rendre inaccessibles.

Précisons toutefois que ce n'est pas la police qui décide, de façon autonome, de bloquer ou non un site web: cette tâche est confiée au ministère public et/ou au juge d'instruction, qui statue au cas par cas.

La Police fédérale possède, au niveau central, une section de quatre personnes dont les tâches sont:

- la gestion de la base de données ICSE;
- l'analyse du matériel saisi (à l'appui des services de recherche fédéraux et locaux);
- la gestion de l'information; le cas échéant, les rapports de police sont redirigés afin d'identifier les suspects et/ou les victimes;
- le cas échéant, l'identification de victimes à la réception des images via Interpol ou directement des services de police membres d'Europol ou Interpol;
- la participation aux groupes d'experts au niveau d'Europol et d'Interpol;
- la représentation de la Police fédérale au sein d'EMPACT Cyber crime/CSE;
- la gestion des dénonciations.

6.3 Fraude en ligne aux cartes de paiement

La fraude en ligne aux cartes de paiement n'est pas suivie au niveau national, ces dossiers sont gérés par la Police fédérale des arrondissements.

Les citoyens et les sociétés privées signalent presque toujours les fraudes aux cartes de paiement à la police (locale) parce que les banques exigent une copie du PV/de la déclaration à la police pour rembourser le montant de la fraude.

La FCCU de la Police fédérale participe au groupe de travail "Internet banking security" qui se penche sur les vulnérabilités et menaces de la fraude à la banque en ligne. Dans le cadre de l'optimalisation de la Police fédérale, il a été décidé qu'il n'y a pas de suivi national concernant les autres formes de fraude à la carte de paiement; ces dossiers sont gérés par les services de la Police fédérale des arrondissements, qui ont également de bons contacts avec l'industrie, mais plutôt au cas par cas.

6.4 Conclusions

La lutte contre la cybercriminalité requiert l'intervention non seulement des forces répressives, mais également celle du secteur privé de la sécurité en matière de sensibilisation et de prévention.
La Belgique a mis en place un CERT pour centraliser les informations concernant les cyberattaques.

Le CCB est l'organe de gouvernance pour les acteurs impliqués dans la lutte contre les cyberincidents (FCCU, RCCU, CERT, SGRS). Il est aussi important de disposer d'une plateforme de concertation et de définir les flux d'informations.

La Belgique est préparée à la lutte contre la pédopornographie, les premières étapes de la localisation de l'infraction étant centralisées auprès de la section Child Abuse de la DSJOC et le dossier étant ensuite transmis aux unités locales compétentes.

Pour une lutte efficace contre la pédopornographie, il est nécessaire d'améliorer le fonctionnement interne de la police, en renforçant les capacités au niveau tant des effectifs que des moyens. De plus, il faut assurer la formation continue des policiers pour renforcer les compétences, élargir les connaissances et partager les expériences vécues.

La lutte contre la pédophilie est du ressort des unités locales, avec l'appui des unités régionales, notamment en ce qui concerne la transmission d'images pédophiles sur l'internet, qui est traitée au sein de la section Child Abuse de la DSJOC, l'enquête étant ensuite confiée aux unités locales compétentes.

Au niveau du ministère public, un rôle de coordination est assigné au procureur général de Liège.

Pour ce qui est des images pédophiles sur l'internet, il existe une unité centrale chargée de les analyser. Si une infraction est constatée, le procès-verbal est adressé au parquet, qui transmet à la police locale pour enquête. Les cas urgents sont toutefois traités par la section Child Abuse de la DSJOC.

Il est prévu d'acquérir des logiciels spécialisés permettant de détecter les images pédophiles. Toutefois, au sein des unités centrales, il existe une pénurie de matériel et de personnes formées.

L'équipe d'évaluation salue les initiatives de la Belgique concernant les campagnes de prévention en concertation avec le secteur privé. Il faut également noter que, pour la prévention du tourisme sexuel, il existe aussi des nombreuses campagnes de prévention et de sensibilisation spécifiques, qui s'adressent aux jeunes.

Un autre aspect positif est le fait d'avoir mis en place la législation nécessaire pour bloquer l'accès aux sites internet ayant des contenus de pédopornographie.

L'équipe d'évaluation observe avec intérêt le projet de loi visant à renforcer le rôle de Child Focus pour la lutte contre la pédopornographie.

En ce qui concerne la fraude en ligne aux cartes de paiement, l'équipe d'évaluation a constaté un manque d'informations sur les résultats des enquêtes qui sont menées par la police locale.

7. COOPÉRATION INTERNATIONALE

7.1 Coopération avec les agences de l'UE

7.1.1 Exigences formelles pour la coopération avec Europol/EC3, Eurojust et l'ENISA

Il n'y a pas de procédures spécifiques pour la coopération en matière de cybercriminalité.

7.1.2 Évaluation de la coopération avec Europol/EC3, Eurojust et l'ENISA

La coopération est évaluée positivement.

La coopération est principalement réalisée par l'activation d'Europol/EC3 dans le cadre d'opérations conjointes. Le rapport IOCTA 2014 a servi à consolider l'approche structurelle au niveau de la Police fédérale.

Les fiches "cyberbits" créées et diffusées par EC3/Europol sont utiles, mais il reste nécessaire d'en effectuer la traduction dans les langues nationales pour en optimaliser l'effet jusque dans les polices locales.

Opération "MOZART"

Courant août 2010, une banque belge était informée par plusieurs de ses clients de ce que leurs sessions de "PC banking" étaient infectées par un virus malveillant (malware). Les pirates informatiques (hackers) avaient tenté de réaliser des virements internationaux vers des comptes bancaires se trouvant en Espagne ou au Portugal. Plainte avait été déposée au Parquet de Bruxelles.

Par la suite, cinq autres banques belges ont également été victimes de virus similaires et ont déposé plainte en 2011 au Parquet de Bruxelles, L'enquête a été diligentée par les services centraux de la Police fédérale.

Le Parquet fédéral a centralisé l'action judiciaire au niveau national et a saisi le juge d'instruction bruxellois Michel Claise le 7/12/2011 du chef de faux informatique, fraude informatique, hacking, et blanchiment commis par des organisations criminelles.

Dans un premier temps, les pirates informatiques collectent les données confidentielles des utilisateurs de systèmes bancaires en ligne dont l'ordinateur est infecté. La récupération des données permet ensuite à ces auteurs d'ouvrir frauduleusement une session bancaire via l'internet à l'insu du client et de transférer de l'argent du compte de la victime vers des comptes bancaires de complices.

Dans un second temps, des complices "money mule" recrutés via courrier électronique par l'organisation criminelle, reçoivent des instructions aux fins de récupérer ces sommes d'argent et de les transférer vers des comptes de tiers se trouvant à l'étranger ("mules de second niveau").

L'action policière coordonnée par la Police fédérale belge a permis l'interpellation de 57 mules de 1er niveau sur le sol belge. Dans le cadre de dossiers distincts, 2 condamnations pour blanchiment sont déjà tombées et 1 mule a fait l'objet d'une transaction pénale.

Les enquêteurs ont mené des investigations dans plusieurs pays (Allemagne, France, Pologne, Lettonie, Estonie, Ukraine, Russie, etc.).

Une opération policière d'envergure, sous l'égide d'Europol, a permis l'arrestation de 7 suspects sur le territoire ukrainien. Parmi ces suspects figurent les deux principaux recruteurs présumés des mules belges.

Grâce à son expertise acquise ces dernières années dans des dossiers similaires de fraudes informatiques, la Police fédérale belge a mis sur pied une équipe "NewTech" composée d'enquêteurs IT spécialisés en cybercriminalité (FCCU) aux côtés d'enquêteurs financiers rompus aux techniques de blanchiment (OCEDEFO).

En date du 7 mars 2013, 5 pays européens (Autriche, Belgique, UK, Finlande et Norvège), rejoints ensuite par les Pays-Bas et soutenus par EUROJUST et EUROPOL, ont signé un protocole d'accord en vue de constituer une Équipe internationale de magistrats et de policiers aux fins d'identifier les organisateurs du piratage des banques européennes.

L'approche de la coopération avec Europol/EC3 est fortement influencée par une culture c*ommon law* où le rôle du ministère public ne reflète pas la réalité pour les dossiers ayant des répercussions au niveau belge. La coopération avec Eurojust est évaluée positivement.

7.1.3 Résultats opérationnels des ECE et des cyberpatrouilles

La Belgique a déjà participé à des ECE dans la lutte contre la cybercriminalité. Ces expériences se sont avérées positives. La Belgique a introduit une demande de financement de l'UE pour des projets IT en matière scientifique (forensique) dans le cadre de l'enveloppe nationale au titre de l'ISF (Fonds pour la sécurité intérieure) de la police et le "Union Action" ensemble avec la France. Ces demandes sont actuellement en attente d'une approbation par la Commission européenne.
La Belgique n'a aucune expérience de la participation à des cyberpatrouilles.

La Belgique suggère une mise en œuvre plus rapide des ECE et considère que le financement de l'UE doit être maintenu. Elle regrette l'absence de financements de l'UE pour la traduction, pourtant souvent indispensables à une bonne collaboration.

7.2 Coopération entre les autorités belges et Interpol

La Police judiciaire fédérale est reliée à l'ICSE depuis 2011. L'accès en est géré par une section spécialisée au niveau de la DJSOC. Une formation spécialisée a été organisée en coopération avec Interpol.

7.3 Coopération avec des pays tiers

Les experts belges mettent leur expertise au service de TAIEX: des experts belges sont mis à la disposition de TAIEX en vue de la formation et de l'augmentation de l'expertise.

Il en va de même pour le Conseil de l'Europe, où des experts belges sont associés à des projets du Conseil, principalement ceux destinés aux pays des Balkans.

En ce qui concerne la coopération à l'échelle européenne, la Belgique fait partie de l'Alliance mondiale contre les abus sexuels commis contre des enfants via Internet, lancée le 5 décembre 2012 et regroupant 53 pays. Cette initiative vise à rassembler les décideurs de l'ensemble de la planète afin de mieux identifier et aider les victimes de ces actes et de poursuivre leurs auteurs. La Belgique est également reliée au système ECRIS (système européen d'information sur les casiers judiciaires) depuis le 2 juillet 2012.

La participation d'Eurojust a certainement apporté une valeur ajoutée dans certains cas concernant des pays tiers, mais Europol/EC3 n'a, à notre sens, apporté aucune plus-value à ce jour.

7.4 Coopération avec le secteur privé

La coopération avec le secteur privé est soutenue. Diverses initiatives ont été lancées, dont les plus importantes sont:

- la collaboration avec le monde universitaire, entamée avec la création du centre d'excellence B-CCENTRE, qui n'est malheureusement plus soutenu;
- la collaboration avec la Fédération des entreprises de Belgique;
- la participation aux initiatives internationales en matière de formation (ECTEG);
- la coopération avec les différentes sociétés de cyber sécurité;
- la collaboration avec le secteur financier suite aux attaques contre les systèmes des banques en ligne.

7.5 Instruments de la coopération internationale

7.5.1 Entraide judiciaire

Il n'existe pas de procédures spécifiques pour la coopération en matière de cybercriminalité. Les dispositions du code de procédure pénale relatives à l'entraide pénale s'appliquent.
La procédure de droit commun s'applique en ce qui concerne la communication de demandes d'entraide judiciaire.

Le Titre III de la Convention de Budapest (Convention sur la cybercriminalité) prévoit, dans le cadre du Conseil de l'Europe, des dispositions en matière d'entraide judiciaire concernant spécifiquement les infractions informatiques au sens large, selon la définition de la Convention de Budapest. Une procédure d'urgence et plusieurs motifs de refus y sont prévus.

Il n'existe pas de fondement juridique spécifique pour l'entraide judiciaire en matière de cybercriminalité. L'article 3 de la loi belge du 9 décembre 2004 sur l'entraide judiciaire internationale en matière pénale et modifiant l'article 90ter du Code d'instruction criminelle (*M.B.* du 24 décembre 2004) dispose que les autorités judiciaires belges accordent l'entraide judiciaire en matière pénale la plus large possible dans le respect de cette loi et des règles de droit international applicables.

On peut renvoyer à la réglementation de droit commun en la matière. En principe, il existe trois possibilités selon la base juridique:

- l'approche traditionnelle, qui intègre les demandes adressées par l'État membre requérant à l'État membre destinataire, le SPF Justice intervenant comme intermédiaire;
- la collaboration au sein de l'espace Schengen et la Convention du 29 mai 2000 au sein de l'Union européenne, qui prévoit la possibilité d'un contact direct entre les autorités judiciaires (bien que chaque État membre reste compétent). De telles requêtes sont transmises directement entre les autorités judiciaires qui sont compétentes territorialement pour l'introduction et l'exécution de ces requêtes;
- la collaboration selon le principe de reconnaissance mutuelle au sein de l'Union européenne, qui implique que les décisions émises dans un État membre de l'Union européenne sont exécutées et reconnues dans un autre État membre de l'UE comme s'il s'agissait de décisions prises par les propres autorités nationales.

Conformément à la loi du 9 décembre 2004, il faut faire une distinction entre les États membres de l'UE et les États tiers.

Art. 5 - L'exécution en Belgique des demandes d'entraide judiciaire en matière pénale transmises par une autorité compétente d'un État membre de l'Union européenne ne nécessite pas l'autorisation préalable du Ministre de la Justice.

Toutefois, si l'exécution d'une demande d'entraide émanant d'une autorité étrangère visée à l'alinéa 1er est susceptible d'être refusée pour un des motifs visés à l'article 4, § 2, alinéa 1er, 1° ou 2°, l'autorité judiciaire qui a reçu la demande transmet celle-ci au ministre de la Justice. Si la demande concernée a été adressée à un procureur du Roi ou à un juge d'instruction, la transmission au ministre de la Justice se fait par l'intermédiaire du procureur général.

Le cas échéant, le ministre de la Justice informe l'autorité requérante qu'il ne peut être donné suite, totalement ou partiellement, à sa demande. Cette information est notifiée à l'autorité judiciaire concernée et fait obstacle à l'exécution de la demande d'entraide ou au retour des pièces d'exécution.

Art. 7. § 1er. Les demandes d'entraide judiciaire en matière pénale émanant des autorités judiciaires belges et destinées aux autorités étrangères compétentes sont transmises, par l'intermédiaire du Service public fédéral Justice, par la voie diplomatique. Le retour des pièces d'exécution se fait par la même voie.

Les demandes d'entraide judiciaire en matière pénale émanant des autorités étrangères compétentes et destinées aux autorités judiciaires belges sont transmises par la voie diplomatique.

Le retour des pièces d'exécution se fait par la même voie.

§ 2. Toutefois, si un instrument international liant l'État requérant et la Belgique le prévoit, les demandes d'entraide judiciaire en matière pénale sont transmises et les pièces d'exécution retournées soit directement entre les autorités judiciaires belges et les autorités étrangères compétentes pour les délivrer et les exécuter, soit entre les départements de la Justice concernés.

§ 3. Une copie de toute demande d'entraide transmise ou reçue par une autorité judiciaire belge est communiquée au Service public fédéral Justice.

§ 4. Lorsque la demande d'entraide judiciaire en matière pénale transmise ou reçue par une autorité judiciaire belge concerne une affaire de nature à troubler gravement l'ordre public ou à porter atteinte à des intérêts essentiels de la Belgique, un rapport d'information est transmis sans délai au Ministre de la Justice par le procureur fédéral ou, lorsqu'un juge d'instruction ou un procureur du Roi est en charge de la demande, par le biais du procureur général. Cette obligation d'information ne préjudicie pas à l'application de l'article 5.

L'autorité centrale de coopération internationale en matière pénale dispose uniquement de chiffres et d'informations sur les demandes d'entraide judiciaire internationale avec des pays non membres de l'UE. Depuis 2004, les demandes d'entraide judiciaire internationale en matière pénale avec des pays membres de l'UE sont directement transmises entre autorités judiciaires, sans intervention du ministère de la Justice. Le principe est de nous transmettre une copie de ces demandes d'entraide judiciaire. Des copies relatives à l'entraide judiciaire, seule est enregistrée une liste d'infractions, sans autre renvoi. Nous ne disposons pas d'autres informations concernant le déroulement ou l'exécution du dossier.

On trouvera ci-après un tableau contenant des données chiffrées en matière de cybercriminalité et de pédopornographie entre pays membres de l'UE.

(Seules ces deux infractions sont enregistrées):

Année	Infraction	De la Belgique	Vers la Belgique
2015	Cybercriminalité	23	38
	Pédopornographie	1	3
2014	Cybercriminalité	61	39
	Pédopornographie	2	7

Dans le tableau ci-dessous, on retrouve des statistiques relatives à la cybercriminalité et à la pédopornographie avec États tiers.
(Seules ces deux infractions sont enregistrées):

Année	Infraction	De la Belgique	Vers la Belgique
2015	Cybercriminalité	8	3
	Pédopornographie	2	1
2014	Cybercriminalité	21	3
	Pédopornographie	0	1

Il n'y a aucune procédure spécifique à suivre ou condition à remplir. La seule remarque à cet égard est que les demandes d'entraide judiciaire avec les États-Unis ne peuvent plus être transmises que par courrier électronique.

En principe, les demandes d'entraide judiciaire doivent être transmises sous format original. En cas d'extrême urgence, une copie peut être fournie à l'autorité centrale, à condition que l'original suive. Le temps de réponse est de 6 mois en moyenne.

7.5.2 Instruments de la reconnaissance mutuelle

En ce qui concerne les instruments de la reconnaissance mutuelle, il faut préciser ce qui suit:

- décision de protection européenne: cette directive n'a pas encore été implémentée. Un avant-projet de loi a déjà été élaboré et sera soumis plus tard cette année au Parlement;
- reconnaissance mutuelle des mesures de contrôle: aucun dossier connu pour les années 2014 et 2015;
- reconnaissance mutuelle des peines d'emprisonnement et des mesures privatives de liberté: deux dossiers sont connus pour 2014. L'un concerne la pédopornographie et l'autre la cybercriminalité;
- reconnaissance et exécution des décisions de confiscation: ces dossiers ne sont pas séparés;
- reconnaissance mutuelle des sanctions pécuniaires: deux dossiers sont connus pour 2014, tous deux en matière de pédopornographie; exécution des décisions de gel d'avoirs ou de preuves: ces dossiers ne sont pas séparés.

7.5.3 Remise/extradition

a) Selon l'article 3 de la loi du 19/12/2003 relative au mandat d'arrêt européen[24], un mandat d'arrêt européen peut être émis pour des faits punis par la loi de l'État membre d'émission d'une peine privative de liberté ou d'une mesure de sûreté privative de liberté d'un maximum d'au moins douze mois ou, lorsqu'une condamnation à une peine est intervenue ou qu'une mesure de sûreté a été infligée, pour autant qu'elles soient d'une durée d'au moins quatre mois.

En ce qui concerne l'exécution d'un mandat d'arrêt européen émanant d'un autre État membre, l'article 5 de la même loi prévoit, en principe, que l'exécution est refusée si le fait qui est à la base du mandat d'arrêt européen ne constitue pas une infraction au regard du droit belge. Cette règle ne s'applique cependant pas si le fait constitue une des infractions suivantes, pour autant qu'il soit puni dans l'État d'émission d'une peine privative de liberté d'un maximum d'au moins trois ans, y inclus pour la cybercriminalité:

b) Selon l'article 1er la loi du 15 mars 1874 sur les extraditions[25], le Gouvernement peut, pour l'exécution des traités conclus avec les États étrangers sur la base de la réciprocité, accorder l'extradition de tout étranger qui, comme auteur, coauteur ou complice, est poursuivi pour une infraction aux lois pénales ou est recherché aux fins d'exécution d'une peine ou d'une mesure de sûreté par les autorités judiciaires de l'État étranger.

Par mesure de sûreté, au sens de la présente loi, on entend toutes mesures privatives de liberté qui ont été ordonnées en complément ou en substitution d'une peine, par sentence d'une juridiction pénale.

[24] M.B. du 22 décembre 2003.
[25] M.B. du 17 mars 1874.

Seuls peuvent cependant donner lieu à extradition, les faits punissables, aux termes de la loi belge et de la loi étrangère, d'une peine privative de liberté dont la durée maximum dépasse un an. Lorsque l'extradition est demandée pour l'exécution d'une peine prononcée, celle-ci doit atteindre une durée d'au moins un an d'emprisonnement. Lorsqu'il s'agit de l'exécution d'une mesure de sûreté, la privation de liberté ordonnée doit être d'une durée indéterminée ou atteindre au moins quatre mois. Lorsque l'infraction, pour laquelle l'extradition est demandée, est punissable de la peine de mort dans l'État requérant, le Gouvernement n'accorde l'extradition que si l'État requérant donne des assurances formelles que la peine de mort ne sera pas exécutée.

Si la demande d'extradition vise plusieurs faits distincts punissables chacun, aux termes de la loi belge et de la loi étrangère, d'une peine privative de liberté mais dont certains ne remplissent pas la condition relative aux taux de la peine, l'extradition peut aussi être accordée pour ces faits même si ceux-ci ont uniquement été sanctionnés par des amendes.

Selon l'article 2 de la loi du 19/12/2003 relative au mandat d'arrêt européen[26], l'arrestation et la remise s'effectuent sur la base d'un mandat d'arrêt européen. Le mandat d'arrêt européen est une décision judiciaire émise par l'autorité judiciaire compétente d'un État membre de l'Union européenne, appelée autorité judiciaire d'émission, en vue de l'arrestation et de la remise par l'autorité judiciaire compétente d'un autre État membre, appelée autorité d'exécution, d'une personne recherchée pour l'exercice de poursuites pénales ou pour l'exécution d'une peine ou d'une mesure de sûreté privative de liberté.

[26] M.B. du 22 décembre 2003.

En ce qui concerne les canaux de communication, les articles 9 et 10 de la même loi prévoient qu'un signalement effectué conformément aux dispositions de l'article 95 de la Convention d'application du 19 juin 1990 de l'Accord de Schengen du 14 juin 1985 relatif à la suppression graduelle des contrôles aux frontières communes vaut mandat d'arrêt européen. Tant que le signalement ne contient pas toutes les informations requises par le mandat d'arrêt européen, le signalement devra être suivi d'une transmission de l'original du mandat d'arrêt européen ou d'une copie certifiée conforme. La personne recherchée peut être arrêtée, sur la base du signalement visé à l'article 9 ou sur production d'un mandat d'arrêt européen.

Conformément à la loi sur les extraditions, le Gouvernement peut accorder l'extradition sur la production soit du jugement ou de l'arrêt de condamnation, soit de l'ordonnance de la chambre du conseil, de l'arrêt de la chambre des mises en accusation ou de l'acte de procédure criminelle, émanant du juge compétent, décrétant formellement ou opérant de plein droit le renvoi du prévenu ou de l'accusé devant la juridiction répressive, délivrés en original ou en expédition authentique.

Elle sera également accordée sur la production du mandat d'arrêt ou de tout autre acte ayant la même force, décerné par l'autorité étrangère compétente, pourvu que ces actes renferment l'indication précise du fait pour lequel ils sont délivrés et qu'ils soient rendus exécutoires par la chambre du conseil du tribunal de première instance du lieu de la résidence de l'étranger en Belgique ou du lieu où il pourra être trouvé.

Les pièces visées aux premier et deuxième alinéas peuvent être produites en télécopie dans les cas où une convention internationale le prévoit expressément et aux conditions d'authentification fixées par celle-ci.

On retrouve ci-après un tableau contenant des données chiffrées en matière de cybercriminalité et de pédopornographie entre pays membres de l'UE.

Année	**Infraction**	**De la Belgique**	**Vers la Belgique**
2015	Cybercriminalité	2	1
	Pédopornographie	/	/
2014	Cybercriminalité	20	/
	Pédopornographie	/	/

Dans le tableau ci-dessous, on trouvera des statistiques relatives à la cybercriminalité et à la pédopornographie avec les États tiers

Année	**Infraction**	**De la Belgique**	**Vers la Belgique**
2015	Cybercriminalité	7	3
	Pédopornographie	/	1
2014	Cybercriminalité	8	11
	Pédopornographie	0	1

Des procédures ou des conditions doivent toujours être respectées, tant pour les remises que pour les extraditions. Nous renvoyons à cet égard à la loi du 19 décembre 2003 relative au mandat d'arrêt européen (M.B. du 22 décembre 2003) et à la loi du 15 mars 1874 sur les extraditions (M.B. du 17 mars 1874).

En ce qui concerne la remise, l'article 10 de la loi du 19 décembre 2003 relative au mandat d'arrêt européen (*M.B*. du 22 décembre 2003) rend l'arrestation possible à partir du moment où la personne recherchée fait l'objet d'un signalement visé à l'article 9 de la même loi.

L'article 5 de la loi du 15 mars 1874 sur les extraditions (*M.B*. du 17 mars 1874) dispose qu'en cas d'urgence, l'étranger pourra être arrêté provisoirement en Belgique, pour l'un des faits mentionnés à l'article 1er de la même loi, sur l'exhibition d'un mandat d'arrêt décerné par le juge d'instruction du lieu de sa résidence ou du lieu où il pourra être trouvé, et motivé sur un avis officiel donné aux autorités belges par les autorités du pays où l'étranger aura été condamné ou poursuivi. Toutefois, dans ce cas, il sera mis en liberté si, dans le délai de quarante jours à dater de son arrestation, il ne reçoit communication du mandat d'arrêt décerné par l'autorité étrangère compétente.

Après l'ordonnance de l'arrestation, le juge d'instruction est autorisé à procéder suivant les règles prescrites par les articles 87 à 90 du code d'instruction criminelle. L'étranger pourra réclamer la liberté provisoire dans le cas où un Belge jouit de cette faculté et sous les mêmes conditions. La demande sera soumise à la chambre du conseil. La chambre du conseil décidera également, après avoir entendu l'étranger, s'il y a lieu ou non de transmettre en tout ou en partie les papiers et autres objets saisis au gouvernement étranger qui demande l'extradition. Elle ordonnera la restitution des papiers et autres objets qui ne se rattachent pas directement au fait imputé au prévenu et statuera, le cas échéant, sur la réclamation des tiers détenteurs ou autres ayants droit.

7.6 Conclusions

La Belgique n'a pas rapporté des difficultés majeures concernant la coopération internationale. La participation aux équipes communes d'enquête est évaluée de manière positive. Il n'y a pas d'expérience en ce qui concerne les cyberpatrouilles.

Les autorités nationales coopèrent étroitement avec Europol/EC3. La Belgique est très impliquée dans le fonctionnement du dispositif européen.

Une formation spécialisée de police a été créée pour travailler avec la base de données ICSE.
Concernant la coopération avec les pays tiers, les autorités nationales n'ont pas fourni d'informations.

La coopération avec le secteur privé est appréciée de manière positive, surtout les collaborations avec le monde universitaire et la Fédération des entreprises de Belgique.

Cependant, la lenteur des procédures d'entraide judiciaire internationale a été stigmatisée par les autorités de police (6 mois en moyenne). Cette situation pourrait être nettement améliorée, surtout au niveau européen, par des procédures allégées pour les informations cruciales, notamment les adresses IP.

8 FORMATION, SENSIBILISATION ET PRÉVENTION

8.1 Formation spécifique

L'Institut de formation judiciaire[27] (IFJ) belge organise différents modules/formations sur la cybercriminalité:

Une ***Formation de base sur la cybercriminalité*** qui vise à sensibiliser les magistrats à la criminalité informatique (*sensu stricto* et *sensu lato*) se déroule en 3 jours. D'une part, elle permet d'acquérir les connaissances techniques nécessaires pour comprendre les dispositions légales en matière de criminalité informatique et les possibilités existant dans le cadre d'une enquête sur des systèmes informatiques. D'autre part, elle permet d'acquérir une image claire des possibilités et limites législatives en matière de répression de la criminalité informatique afin de les appliquer dans la pratique de manière efficace.

Cette formation s'adresse au public suivant:

- les magistrats qui entrent régulièrement en contact avec certains aspects de la cyberrecherche;
- les magistrats des cours d'appel et des tribunaux de première instance siégeant dans des affaires correctionnelles, ainsi que les juges d'instruction et les magistrats de parquet;
- les stagiaires judiciaires de deuxième année, pour qui cette formation est obligatoire;
- les juristes de parquet;
- les magistrats du ministère public récemment nommés (depuis le 1er janvier 2014) sur la base de la réussite de l'examen concernant la compétence professionnelle ou d'un examen d'évaluation orale, pour qui la participation à cette édition est obligatoire dans le cadre de leur formation initiale.

[27] http://www.igo-ifj.be/fr

- Depuis 2015, l'IFJ a développé une ***Formation spécialisée sur la cybercriminalité***, qui s'adresse particulièrement aux magistrats, stagiaires judiciaires et juristes de parquet qui disposent du certificat de la ***Formation de base sur la cybercriminalité***, ainsi qu'aux magistrats fédéraux. La formation spécialisée se déroule en 2 jours et vient renforcer les connaissances de base acquises lors de la formation initiale sur la cybercriminalité. Elle permet d'acquérir une connaissance approfondie sur l'utilisation des médias sociaux dans les enquêtes proactives et réactives pénales, l'utilisation des méthodes de recherche particulières dans un entourage virtuel, la coopération internationale en matière pénale (en particulier avec les USA), plus particulièrement en ce qui concerne les traces et les preuves numériques, ainsi que sur les compétences et juridictions territoriales dans le cyberespace.

- Un module spécialisé d'une demi-journée de ***Formation sur la coopération internationale avec les États-Unis afin d'obtenir des données de communication des fournisseurs américains*** est également organisé pour les magistrats (fédéraux ou spécialisés en terrorisme), les stagiaires judiciaires et experts juridiques des bureaux de procureurs depuis 2015. Il s'agit d'une table ronde spécialisée sur l'obtention de l'assistance juridique internationale des USA et des prestataires de services américains; l'obtention des données (contenu, données du trafic, informations d'abonné) des services de communication en ligne basés aux USA (WhatsApp, Skype, Facebook, Google, YouTube, Yahoo, etc.) ainsi qu'un débat ouvert sur des dossiers particuliers, en présence de spécialistes du ministère de la Justice des USA.

En ce qui concerne les services de police, diverses formations sont également organisées:

- La formation des policiers "premiers intervenants" des polices locales fait l'objet d'un projet de formation au format "apprentissage en ligne" qui aboutira à un guide de référence disponible pour identifier et saisir les objets pouvant contenir des traces informatiques ainsi que pour entendre les victimes d'une criminalité non spécifique commise par l'utilisation des nouvelles technologies.
- Les enquêteurs des polices locales et fédérale consacrent, lors de leur formation, 12 heures aux nouvelles formes de criminalité et aux possibilités d'enquête.
- Les enquêteurs spécialisés des RCCU et de la FCCU reçoivent une formation de 120 heures, dont 90 heures sur les pratiques technico-légales et 30 heures sur les dispositions du cadre légal et la coopération internationale. Après cette formation de base, organisée en principe annuellement, ils sont appelés à suivre des formations intermédiaires et avancées, données en interne ou dans le cadre de projets financés par des subsides européens (OLAF, cours pilotes ECTEG, etc.). Il n'existe pas de ressource budgétaire spécifiquement affectée aux formations "cyber" et les formations disponibles nécessitant une contribution financière sont suivies en fonction du budget libéré, au cas par cas, en favorisant une approche consistant à "former les formateurs".

Des formations en audit sécurité IT, comportant les réactions à avoir en cas d'incident, sont également proposées par des établissements tels que la Solvay Brussels School, et l'ICHEC ainsi que dans diverses hautes écoles, telles que l'HOWEST et l'ESI, et universités telles que Namur (FUNDP), Leuven (KULeuven) et Gand (Gent).

Aucune certification des connaissances des experts judiciaires n'est actuellement requise, le simple fait d'être désigné comme expert par un juge suffit.

La FCCU coordonne les formations et les organise sur la base des besoins exprimés par les praticiens et en tenant compte des expertises communiquées par les partenaires du monde universitaire, d'Europol, d'Interpol et des homologues au niveau de l'UE, entre autres au sein du groupe ECTEG.

Les formations de base technico-légale et "cyber" sont le résultat de la transposition du matériel disponible auprès de l'ECTEG, certains membres de la FCCU/des RCCU apportant également leur contribution en tant qu'experts pour les mises à jour.

La formation de base dispensée par EC3/Europol est l'occasion d'assurer une formation de base, complémentaire aux formations existantes et constitue une excellente opportunité de mettre en réseau les praticiens.

Dans la mesure où des places sont disponibles dans les formations données en Belgique par la FCCU, en interne ou en collaboration avec le B-CCENTRE, celles-ci sont ouvertes aux pays tiers, en tenant compte de la langue du cours et de son sujet.

En ce qui concerne la Police fédérale, il s'agit principalement du coût lié à l'engagement du personnel spécialisé qui contribue à l'élaboration et à la distribution de ces formations. Il n'y a pas d'enveloppe spécifique dédiée, au sein de la Police fédérale judiciaire, aux formations externes au profit des spécialistes en cybercriminalité. Le coût moyen annuel s'élève à 22 000 euros. En 2015, un budget spécifique "one shot" pour la lutte contre le terrorisme a été partiellement consacré aux formations, surtout en matière d'analyse technico-légale des appareils mobiles (smartphones, tablettes) à hauteur de 20 000 euros pour des formations de 4 personnes, chargées de déployer cette formation au niveau national.

Des formations ont été organisées par le Centre d'excellence belge, le B-CCENTRE, au profit des enquêteurs spécialisés des RCCU et de la FCCU.

A la fin du projet B-CCENTRE financé par les fonds européens, la carence d'un financement structurel national, par exemple sur fonds ISF, a empêché la poursuite de ce partenariat.

Diverses formations sont disponibles dans le monde universitaire sous la forme d'années de spécialisation en cybersécurité, incorporées au cursus de bachelier et de master.

Dans ces cursus, des intervenants de la FCCU sont appelés à transmettre les éléments essentiels en matière de réaction en cas d'incident et de préservation des traces informatiques.

8.2 Sensibilisation

Diverses initiatives, soit au niveau étatique, soit au niveau privé, sont prises pour sensibiliser au problème de la cybercriminalité.

8.3 Prévention

Bien qu'il existe diverses initiatives, les interlocuteurs ont précisé que les moyens sont insuffisants pour offrir une réponse adaptée au phénomène de la cybercriminalité. Afin d'éviter que les différents acteurs entre en concurrence, une gouvernance centrale devra être mise en place, tâche qui pourrait être confiée au nouveau CCB.

8.3.1 Législation/politique nationale et autres mesures

Le CERT.be a un rôle important à jouer dans le cadre de la prévention. En tant qu'expert en sécurité sur l'internet et les réseaux, le CERT.be entend aider les entreprises, ainsi que d'autres organisations, à coordonner, résoudre et prévenir les problèmes de sécurité. Il faut quand même préciser que le CERT axe ses interventions concrètes en cas d'incidents cyber sur les infrastructures critiques. L'aide aux entreprises est donc très limitée, et uniquement si les ressources sont disponibles.

Le faible niveau de sensibilisation chez les utilisateurs finals accroît les risques. Ainsi, les collaborateurs compromettent régulièrement la sécurité des systèmes IT sans s'en rendre compte, par exemple en travaillant sur un appareil non protégé, en communiquant un mot de passe en toute bonne foi, en réutilisant des mots de passe faibles ou en cliquant sur un lien dans un courrier électronique d'hameçonnage (phishing). Les utilisateurs qui travaillent sans logiciels de protection ou avec des versions obsolètes de ceux-ci peuvent également causer des problèmes à votre entreprise. Voilà pourquoi le CERT.be s'adresse aussi aux utilisateurs individuels, pour lesquels il établit des campagnes de sensibilisation.

Les malwares ou logiciels malveillants utilisés par les criminels sont de plus en plus difficiles à neutraliser. Certains possèdent même leur propre mécanisme de défense. Le CERT.be recueille automatiquement des informations sur les menaces et incidents par le biais de capteurs, de honeypots (systèmes de leurre) et d'autres systèmes. Les services proactifs du CERT sont axés sur la prévention des cyberincidents et la limitation de leur impact, le cas échéant. Dans le moyen et le long terme, nous nous efforçons d'améliorer la protection des infrastructures IT par divers moyens:

- publication d'informations et de conseils sur la protection;
- suivi et évaluation des tendances et des technologies;
- sensibilisation des spécialistes et des utilisateurs de systèmes IT;
- partage de connaissances et d'informations;
- organisation de conférences et d'ateliers spécialisés.

Dernièrement, en octobre 2015, une campagne de sensibilisation, née de la collaboration du CERT et de la "cyber-security coalition", a été lancée en Belgique avec pour objectif l'utilisation de phrases en lieu et place de mots en guise de mot de passe (cf. www.safeonweb.be). La "cyber-security coalition" a également une mission de sensibilisation.

8.3.2 Partenariat public/privé (PPP)

En 2014, à l'initiative d'acteurs privés (l'opérateur historique de télécommunications, des sociétés d'audit, etc.) et de partenaires du monde universitaire et gouvernemental (B-CCENTRE, CERT, FCCU, etc.), la création de la Cyber Security Coalition a mis en œuvre des chantiers en matière de sensibilisation, de bonnes pratiques et de formations (à l'attention des managers).

La coopération avec Child Focus est momentanément sujette à discussion. Les parties autour de la table (le ministère de la Justice, les autorités judiciaires et la police) sont en train d'examiner comment développer le rôle de Child Focus, sans sortir du terrain attribué au secteur privé.

8.4 Conclusions

L'équipe d'évaluation a fait le constat qu'au niveau de la police, certaines zones de police créent également leur "Local CCU", soit en débauchant des membres de la RCCU, soit en attribuant cette fonction à des volontaires dotés de connaissances empiriques.

En absence de formation spécifique, ces intervenants effectuent des analyses non conformes aux bonnes pratiques et peuvent mettre en cause la validité de la preuve devant les tribunaux. L'équipe d'évaluation suggère que la formation devrait être centralisée et coordonnée au niveau de la FCCU.

Les formations proposées par des sociétés privées sont très coûteuses et inabordables avec le budget de formation externe de 3 000 € par an dont disposent le FCCU et toutes les RCCU.

Concernant la prévention et la sensibilisation, les moyens employés sont insuffisants pour offrir une réponse adéquate.

Les formations spécialisées pour les magistrats ont débuté en 2004 et elles sont devenues obligatoires, seulement pour les nouveaux magistrats, à partir de 2013.

En 2015, 55 magistrats ont suivi la formation sur la cybercriminalité et 33 magistrats celle sur la coopération avec les États-Unis. Le problème principal reste néanmoins le manque de formation des juges recrutés avant 2013, y compris aussi en raison d'une certaine réticence des juges à s'investir dans la formation (il a été indiqué que les juges ne peuvent pas s'absenter des tribunaux pendant deux ou trois jours pour se rendre à Bruxelles à l'Institut de formation judiciaire (IFJ)).

En 2015, de nouvelles formations ont été élaborées en matière de cybercriminalité (très bien structurée, deux journées de cours) et de coopération avec les États-Unis.

Il conviendrait de suggérer à la Belgique de renforcer la formation des juges dans le domaine de la cybercriminalité.

9 REMARQUES FINALES ET RECOMMANDATIONS

9.1. Suggestions de la Belgique

- La création d'un modèle de référence au niveau de l'UE, définissant des standards en matière de structure et de fonctionnement des unités d'enquête sur la cybercriminalité et prévoyant des normes minimales permettrait d'améliorer le fonctionnement au niveau national et l'intégration des acteurs lorsque le phénomène revêt un aspect international.

- La mise à disposition de normes, telles que le Guide sur la preuve électronique rédigé par le Conseil de l'Europe, combinée au projet EVIDENCE pour soutenir l'effort de recherche de qualité dans la collecte et la gestion de la preuve.

- L'utilisation d'une taxonomie commune (projet ENISA), couplée à un outil statistique similaire dans l'ensemble des pays permettrait d'obtenir un meilleur état de la situation, en temps réel, des phénomènes et par là même de fournir au monde politique un critère d'appréciation utile.

- L'orientation des attributions des fonds ISF ne couvre plus les tâches qui, auparavant, étaient soutenues par les fonds de l'UE. Ces tâches restent nécessaires, notamment en ce qui concerne la création et le fonctionnement de partenariats public/privé, avec l'industrie mais également avec le monde universitaire. L'importance de ces partenariats n'est plus à démontrer en matière de sensibilisation, de formations et de recherche et développement.

- Une approche de certification des entités d'analyse, couvrant tant les procédures que les praticiens, et s'appuyant sur une validation des outils logiciels utilisés permettrait d'améliorer la qualité de la preuve technico-légale dans le domaine des nouvelles technologies. La définition de standards au niveau européen, à défaut du niveau mondial, faciliterait la coopération judiciaire dans les dossiers de dimension transnationale et l'échange de connaissances et de méthodes entre les praticiens.

9.2 Recommandations

18 mois après l'évaluation, la Belgique devrait procéder à un suivi des recommandations figurant dans le présent rapport et rendre compte des progrès effectués au groupe "Questions générales, y compris l'évaluation" (GENVAL).

L'équipe d'évaluation a jugé opportun d'adresser un certain nombre de suggestions aux autorités belges. Elle a en outre présenté, sur la base des différentes bonnes pratiques, des recommandations à l'UE ainsi qu'à ses institutions et agences, et notamment à Europol.

9.2.1 Recommandations à la Belgique

La Belgique devrait:

1. poursuivre les efforts en vue d' unifier le système de collecte des statistiques et d'utiliser une taxonomie commune pour tous les acteurs;

2. finaliser la mise en place du CCB par un recrutement adéquat de moyens humains et renforcer le rôle de cette structure sur le plan de la coordination de la cybersécurité;

3. renforcer le budget dédié aux structures de lutte contre la cybercriminalité (ressources humaines, moyens, formation);

4. clarifier davantage les compétences des différentes structures de la police qui ont des missions de lutte contre la cybercriminalité;

5. renforcer les règles législatives et procédurales concernant les investigations en sources ouvertes;

6. renforcer la formation des magistrats en matière de cybercriminalité;

9.2.2 Recommandations à l'Union européenne, à ses institutions et aux autres États membres

Au niveau de l'Union européenne, l'équipe d'évaluation considère utile de prendre en considération:

- de simplifier les procédures d'entraide judiciaire entre les différents États membres pour faciliter et accélérer l'échange d'informations;

- de proposer un nouveau projet de directive relative à la conservation des données;

- d'uniformiser les règles procédurales concernant la preuve numérique et de développer la reconnaissance mutuelle immédiate;

- d'adopter des règles concernant l'obligation pour les entreprises de communiquer des données aux autorités judiciaires si les services sont fournis en Europe (doctrine Yahoo).

Les États membres devraient approfondir les bonnes pratiques identifiées en Belgique, à savoir:

1. la spécialisation du parquet, par la création d'un réseau d'expertise en cybercriminalité, dont le coordinateur est le Parquet général d'Anvers;

2. la structure et la qualité de la formation sur la cybercriminalité offerte par l'Institut de formation judiciaire;

3. l'activité de la société civile (Child Focus) dans le domaine de la prévention et son implication dans la lutte contre la pédophilie;

ANNEXE A: PROGRAMME DE LA VISITE SUR PLACE

7me série d'évaluations mutuelles du GENVAL du Conseil de l'Union européenne

Mise en œuvre pratique et fonctionnement des politiques européennes

en matière de prévention de la cybercriminalité et de lutte contre celle-ci

Programme de la visite sur place en Belgique du 26 au 28 avril 2016

Lundi 25 avril 2016

Arrivée des participants

Mardi 26 avril 2016

9h30:

Visite au

SPF Justice (*Boulevard de Waterloo 115, 1000 Bruxelles)*

Sujets: mots de bienvenue, cadre législatif, priorités politiques, rôle des acteurs dans la lutte contre la cybercriminalité

Participants:

- Représentants du SPF Justice
- Représentants de la cellule stratégique du ministre de la Justice
- Juge d'instruction
- Parquet fédéral
- Parquet général
- Police fédérale
- Centre pour la cybersécurité Belgique

12h30: Déjeuner

14h00-17h00:

Visite au Parquet fédéral (*Rue aux Laines 66, 1000 Bruxelles)*

Sujets: Fonctionnement dans le cadre de la lutte contre la cybercriminalité (y compris les cyberattaques, les abus sexuels/la pornographie en ligne impliquant des enfants, ainsi que la cyber fraude aux cartes de crédit)

Participants:

- Réseau d'expertise du Collège des procureurs généraux
- Parquet fédéral
- Juge d'instruction

Mercredi 27 avril 2016

9h00: Visite à la Police fédérale *(RAC, Rue Royale 202A, 1000 Bruxelles)*

Sujet: la lutte contre la cybercriminalité

Participants:

- FGP Anvers RCCU
- FCCU

12h00: Déjeuner

13h00-17h00: Sujets: les abus sexuels/la pornographie en ligne impliquant des enfants, des recherches sur l'internet et la cybersécurité

Participants:

- Police fédérale;
- Centre pour la cybersécurité Belgique
- CERT
- CYBER SECURITY COALITION

Jeudi 28 avril 2016

9h30: Visite à l'Institut de formation judiciaire (*Avenue Louise 54, 1000 Bruxelles)*

Sujet: formations

Participants:

- Parquet fédéral
- Juge d'instruction
- Police fédérale
- Institut de formation judiciaire

12h30: Déjeuner

13h30-16h30: Sujet: relations Europol/Eurojust

Sujet: débat général, questions-réponses

ANNEXE B: PERSONNES RENCONTRÉES

Personnes rencontrées	Organisation
Daniel Flore	Directeur général de la Direction générale de la Législation, des Libertés et Droits Fondamentaux, Service Public Fédéral Justice
Stéphanie Bosly	Chef de service du droit pénal européen, SPF Justice
Frederik Decruyenaere	Chef de service des infractions et procédures particulières, SPF Justice
Claire Huberts	Attachés au service des principes de droit pénal et de la procédure pénale, SPF Justice
Nathalie Cloosen	Attachés au service du droit pénal européen, SPF Justice
Serge De Biolley	Représentant de la cellule stratégique du Ministre de la Justice
Geert Schoorens	Parquet fédéral
Dirk Schoeters	Parquet-général d'Anvers
Yves Vandermeer	Police fédérale

Mercredi 27 avril 2016 - Visite à la Police fédérale

Personnes rencontrées	Organisation
Johan Van Den Berghe	Police fédérale Anvers – RCCU
Walter Coenraets	Police fédérale – DJSOC/FCCU
Yves Vandermeer	Police fédérale – DJSOC/FCCU
Marjolein Delplace	Police fédérale – DJSOC/Stratégie & PNS
Christine Casteels	Police fédérale – DJSOC/Stratégie & PNS
Yves Goethals	Police fédérale – DJSOC/Child Abuse
Elrik Robbe	Police fédérale – DJSOC/Recherche Internet
Didier Louis	Police fédérale Bruxelles – Child abuse
Vanessa Hubert	Police locale – ZP Montgomery – Child abuse
Peter Gouwy	Europol
Phédra Clouner	Cyber Security Centre Belgium
Geert Schoorens	Parquet fédéral
Nathalie Dewancker	Cyber Security Coalition
Nathalie Cloosen	SPF Justice

Jeudi 28 avril 2016 – Visite à l'institut de formation judiciaire

Personnes rencontrées	Organisation
Jan Kerkhofs	Parquet fédéral
Philippe Van Linthout	Juge d'instruction Malines
Dirk Schoeter	Parquet-général d'Anvers
Jos De Vos	Institut de formation judiciaire
Meta Lubambu	Institut de formation judiciaire
Yves Vandermeer	Police fédérale
Nathalie Cloosen	SPF Justice

ANNEXE C: LISTE DES ABRÉVIATIONS/GLOSSAIRE DES TERMES UTILISÉS

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	FRENCH OR ACRONYM IN ORIGINAL LANGUAGE	FRENCH OR ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
B-CCENTRE		Plateforme de concertation relative à la sécurité des réseaux informatiques	Belgian Cybercrime Centre of Excellence for Training, Research & Education BelNIS
CCB	Centre pour la cybersécurité Belgique		
CCU			Computer Crime Unit
CERT			Federal Cyber Emergency Team
CIC	Code d'instruction criminelle		
DJSOC	Police judiciaire fédérale - Direction de la lutte contre la criminalité grave et organisée		
ECE	Équipes communes d'enquête		
FEB	Fédération des entreprises de Belgique		
FEDICT	Service public fédéral Technologie de l'information et de la communication		
FCCU			Federal Computer Crime Unit

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	FRENCH OR ACRONYM IN ORIGINAL LANGUAGE	FRENCH OR ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
IBPT	Institut belge des services postaux et des télécommunications		
IFJ	Institut de formation judiciaire		
LCCU			Local Computer Crime Unit
RCCU	CCU régionale		
SGRS	Service général du renseignement et de la sécurité		
SPF	Service public fédéral		

ANNEXE D: LA LÉGISLATION PERTINENTE

Art. 550bis du Code pénal: "§1er.Celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient, est puni d'un emprisonnement de trois mois à un an et d'une amende de vingt-six [euros] à vingt-cinq mille [euros] ou d'une de ces peines seulement. Si l'infraction visée à l'alinéa 1er, est commise avec une intention frauduleuse, la peine d'emprisonnement est de six mois à deux ans. § 2. Celui qui, avec une intention frauduleuse ou dans le but de nuire, outrepasse son pouvoir d'accès à un système informatique, est puni d'un emprisonnement de six mois à deux ans et d'une amende de vingt-six [euros] à vingt-cinq mille [euros] ou d'une de ces peines seulement. § 3. Celui qui se trouve dans une des situations visées aux §§ 1er et 2 et qui:1° soit reprend, de quelque manière que ce soit, les données stockées, traitées ou transmises par le système informatique; 2° soit fait un usage quelconque d'un système informatique appartenant à un tiers ou se sert du système informatique pour accéder au système informatique d'un tiers; 3° soit cause un dommage quelconque, même non intentionnellement, au système informatique ou aux données qui sont stockées traitées ou transmises par ce système ou au système informatique d'un tiers ou aux données qui sont stockées, traitées ou transmises par ce système; est puni d'un emprisonnement de un à trois ans et d'une amende de vingt-six [euros] belges à cinquante mille [euros] ou d'une de ces peines seulement. § 4. La tentative de commettre une des infractions visées aux §§ 1er et 2 est punie des mêmes peines. § 5. (Celui qui, indûment, possède, produit, vend, obtient en vue de son utilisation, importe, diffuse ou met à disposition sous une autre forme, un quelconque dispositif, y compris des données informatiques, principalement conçu ou adapté pour permettre la commission des infractions prévues au §§ 1er à 4, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à cent mille euros ou d'une de ces peines seulement.).§ 6. Celui qui ordonne la commission d'une des infractions visées aux §§ 1er à 5 ou qui y incite, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de cent [euros] à

deux cent mille [euros] ou d'une de ces peines seulement. § 7. Celui qui, sachant que des données ont été obtenues par la commission d'une des infractions visées aux §§ 1er à 3, les détient, les révèle à une autre personne ou les divulgue, ou fait un usage quelconque des données ainsi obtenues, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six [euros] à cent mille [euros] ou d'une de ces peines seulement. § 8. Les peines prévues par les §§ 1er à 7 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans qui suivent le prononcé d'une condamnation pour une de ces infractions ou pour une des infractions visées aux articles 210bis, 259bis, 314bis, 504quater ou 550ter".

Art. 550ter du Code pénal: "§1er. (Celui qui, sachant qu'il n'y est pas autorisé, directement ou indirectement, introduit dans un système informatique, modifie ou efface des données, ou qui modifie par tout moyen technologique l'utilisation normale de données dans un système informatique, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à vingt-cinq mille euros ou d'une de ces peines seulement. Si l'infraction visée à l'alinéa 1er est commise avec une intention frauduleuse ou dans le but de nuire, la peine d'emprisonnement est de six mois à cinq ans.) . § 2. Celui qui, suite à la commission d'une infraction visée au § 1er, cause un dommage à des données dans le système informatique concerné ou dans tout autre système informatique, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de vingt-six [euros] à septante-cinq mille [euros] ou d'une de ces peines seulement. § 3. Celui qui, suite à la commission d'une infraction visée au § 1er, empêche, totalement ou partiellement, le fonctionnement correct du système informatique concerné ou de tout autre système informatique, est puni d'un emprisonnement de un an à cinq ans et d'une amende de vingt-six [euros] à cent mille [euros] ou d'une de ces peines seulement. § 4. (Celui qui, indûment, possède, produit, vend, obtient en vue de son utilisation, importe, diffuse ou met à disposition sous une autre forme, un dispositif y

compris des données informatiques, principalement conçu ou adapté pour permettre la commission des infractions prévues au §§ 1er à 3, alors qu'il sait que ces données peuvent être utilisées pour causer un dommage à des données ou empêcher, totalement ou partiellement, le fonctionnement correct d'un système informatique, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à cent mille euros ou d'une de ces peines seulement.). § 5. Les peines prévues par les §§ 1er à 4 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans qui suivent le prononcé d'une condamnation pour une de ces infractions ou pour une des infractions visées aux articles 210bis, 259bis, 314bis, 504quater ou 550bis. (§ 6. La tentative de commettre l'infraction visée au § 1er est punie des mêmes peines.)".

Art. 550ter du Code pénal: "§ 1er. (Celui qui, sachant qu'il n'y est pas autorisé, directement ou indirectement, introduit dans un système informatique, modifie ou efface des données, ou qui modifie par tout moyen technologique l'utilisation normale de données dans un système informatique, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à vingt-cinq mille euros ou d'une de ces peines seulement.

Si l'infraction visée à l'alinéa 1er est commise avec une intention frauduleuse ou dans le but de nuire, la peine d'emprisonnement est de six mois à cinq ans.). § 2. Celui qui, suite à la commission d'une infraction visée au § 1er, cause un dommage à des données dans le système informatique concerné ou dans tout autre système informatique, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de vingt-six [euros] à septante-cinq mille [euros] ou d'une de ces peines seulement. § 3. Celui qui, suite à la commission d'une infraction visée au § 1er, empêche, totalement ou partiellement, le fonctionnement correct du système informatique concerné ou de tout autre système informatique, est puni d'un emprisonnement de un an à cinq ans et d'une amende de vingt-six [euros] à cent mille [euros] ou d'une de ces peines seulement.

§ 4. (Celui qui, indûment, possède, produit, vend, obtient en vue de son utilisation, importe, diffuse ou met à disposition sous une autre forme, un dispositif y compris des données informatiques, principalement conçu ou adapté pour permettre la commission des infractions prévues au §§ 1er à 3, alors qu'il sait que ces données peuvent être utilisées pour causer un dommage à des données ou empêcher, totalement ou partiellement, le fonctionnement correct d'un système informatique, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à cent mille euros ou d'une de ces peines seulement.) § 5. Les peines prévues par les §§ 1er à 4 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans qui suivent le prononcé d'une condamnation pour une de ces infractions ou pour une des infractions visées aux articles 210bis, 259bis, 314bis, 504quater ou 550bis. (§ 6. La tentative de commettre l'infraction visée au § 1er est punie des mêmes peines.)

Art. 259bis. du Code pénal: "§ 1. Sera puni d'un emprisonnement de six mois à deux ans et d'une amende de cinq cents [euros] à vingt mille [euros] ou d'une de ces peines seulement, tout officier ou fonctionnaire public, dépositaire ou agent de la force publique qui, à l'occasion de l'exercice de ses fonctions, hors les cas prévus par la loi ou sans respecter les formalités qu'elle prescrit: 1° soit, intentionnellement, à l'aide d'un appareil quelconque, écoute ou fait écouter, prend connaissance ou fait prendre connaissance, enregistre ou fait enregistrer, pendant leur transmission, des communications ou des télécommunications privées, auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications ou télécommunications; 2° soit, avec l'intention de commettre une des infractions mentionnées ci-dessus, installe ou fait installer un appareil quelconque; 3° soit, sciemment, détient, révèle ou divulgue à une autre personne le contenu de communications ou de télécommunications privées, illégalement écoutées ou enregistrées, ou dont il a pris connaissance illégalement, ou utilise sciemment d'une manière quelconque une information obtenue de cette façon.

§ 2. Sera puni d'un emprisonnement de six mois à trois ans et d'une amende de cinq cents [euros] à trente mille [euros] ou d'une de ces peines seulement, tout officier ou fonctionnaire public, dépositaire ou agent de la force publique qui, à l'occasion de l'exercice de ses fonctions, hors les cas prévus par la loi ou sans respecter les formalités qu'elle prescrit, avec une intention frauduleuse ou à dessein de nuire, utilise un enregistrement, légalement effectué, de communications ou de télécommunications privées. [§ 2bis. Sera puni d'un emprisonnement de six mois à deux ans et d'une amende de cinq cents euros à vingt mille euros ou d'une de ces peines seulement, tout officier ou fonctionnaire public, dépositaire ou agent de la force publique qui, à l'occasion de l'exercice de ses fonctions, hors les cas prévus par la loi ou sans respecter les formalités qu'elle prescrit, indûment, possède, produit, vend, obtient en vue de son utilisation, importe, diffuse ou met à disposition sous une autre forme un dispositif, y compris des données informatiques, principalement conçu ou adapté pour permettre la commission de l'infraction prévue au § 1er.] § 3. La tentative de commettre une des infractions visées aux [§§ 1er, 2 ou 2bis] est punie comme l'infraction elle-même. § 4. Les peines [prévues aux §§ 1er à 3] sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans à compter du prononcé d'un jugement ou d'un arrêt, passés en force de chose jugée, portant condamnation en raison de l'une de ces infractions ou de l'une des infractions visées [à l'article 314bis, §§ 1er à 3]. § 5. [Les dispositions du § 1er, 1° et 2°, ne s'appliquent pas à [1 la recherche]1 la captation, l'écoute, la prise de connaissance ou l'enregistrement, par le Service Général du Renseignement et de la Sécurité des Forces armées de toute forme de communications émises à l'étranger tant à des fins militaires dans le cadre des missions explicitées à l'article 11, § 2, 1° et 2° de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité que pour des motifs de sécurité et de protection de nos troupes et de celles de nos alliés lors de missions à l'étranger et de nos ressortissants établis à l'étranger, comme explicité au même article 11, § 2, 3° et 4°.] ».

Art. 314bis. du Code pénal: "§ 1. Sera puni d'un emprisonnement de six mois à un an et d'une amende de deux cents [euros] à dix mille [euros] ou d'une de ces peines seulement, quiconque: 1° soit, intentionnellement, à l'aide d'un appareil quelconque, écoute ou fait écouter, prend connaissance ou fait prendre connaissance, enregistre ou fait enregistrer, pendant leur transmission, des communications ou des télécommunications privées, auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications ou télécommunications; 2° soit, avec l'intention de commettre une des infractions mentionnées ci-dessus, installe ou fait installer un appareil quelconque.§ 2. Sera puni d'un emprisonnement de six mois à deux ans et d'une amende de cinq cents [euros] à vingt mille [euros] ou d'une de ces peines seulement, quiconque détient, révèle ou divulgue sciemment à une autre personne le contenu de communications ou de télécommunications privées, illégalement écoutées ou enregistrées, ou dont il a pris connaissance illégalement, ou utilise sciemment d'une manière quelconque une information obtenue de cette façon. Sera puni des mêmes peines quiconque, avec une intention frauduleuse ou à dessein de nuire, utilise un enregistrement, légalement effectué, de communications ou de télécommunications privées. (§ 2bis. Sera puni d'un emprisonnement de six mois à un an et d'une amende de deux cents euros à dix mille euros ou d'une de ces peines seulement, celui qui, indûment, possède, produit, vend obtient en vue de son utilisation, importe, diffuse ou met à disposition sous une autre forme un dispositif, y compris des données informatiques, principalement conçu ou adapté pour permettre la commission de l'infraction prévue au § 1er.) § 3. La tentative de commettre une des infractions visées aux (§§ 1er, 2 ou 2bis) est punie comme l'infraction elle-même. § 4. Les peines (prévues aux §§ 1er à 3) sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans à compter du prononcé d'un jugement ou d'un arrêt, passés en force de chose jugée, portant condamnation en raison de l'une de ces infractions ou de l'une des infractions visées (à l'article 259bis, §§ 1er à 3)."

CHAPITRE V. - DE L'ATTENTAT A LA PUDEUR ET DU VIOL.

Art. 372. du Code pénal: "Tout attentat à la pudeur commis sans violences ni menaces sur la personne ou à l'aide de la personne d'un enfant de l'un ou de l'autre sexe, âgé de moins de seize ans accomplis, sera puni de la réclusion (de cinq ans à dix ans). (Sera puni de la réclusion de dix à quinze ans l'attentat à la pudeur commis, sans violences ni menaces, par tout ascendant ou adoptant sur la personne ou à l'aide de la personne d'un mineur, même âgé de seize ans accomplis, mais non émancipé par le mariage. (La même peine sera appliquée si le coupable est soit le frère ou la sœur de la victime mineure ou toute personne qui occupe une position similaire au sein de la famille, soit toute personne cohabitant habituellement ou occasionnellement avec elle et qui a autorité sur elle.)

Art. 373. du Code pénal: "L'attentat à la pudeur, commis avec violences ou menaces, sur des personnes de l'un ou de l'autre sexe, sera puni d'un emprisonnement de six mois à cinq ans. Si l'attentat a été commis sur la personne d'un mineur de plus de seize ans accomplis, le coupable subira la réclusion (de cinq ans à dix ans). La peine sera (de la réclusion) de dix à quinze ans, si le mineur était âgé de moins de seize ans accomplis."

Art. 374. du Code pénal: "L'attentat existe dès qu'il y a commencement d'exécution."

Art. 375. du Code pénal: "(Tout acte de pénétration sexuelle, de quelque nature qu'il soit et par quelque moyen que ce soit, commis sur une personne qui n'y consent pas, constitue le crime de viol. Il n'y a pas consentement notamment lorsque l'acte a été imposé par violence, contrainte ou ruse, ou a été rendu possible en raison d'une infirmité ou d'une déficience physique ou mentale de la victime.) (Quiconque aura commis le crime de viol sera puni de réclusion de cinq ans à dix ans.) (Si le crime a été commis sur la personne d'un mineur âgé de plus de seize ans accomplis, le coupable sera puni de la peine de la réclusion de dix à quinze ans.) (Si le crime a été commis sur la personne d'un enfant âgé de plus de quatorze ans accomplis et de moins de seize ans accomplis, le coupable sera puni de la peine de la réclusion de quinze à vingt ans.) (Est réputé viol à l'aide de violences tout acte de pénétration sexuelle, de quelque nature qu'il soit et par quelque moyen que ce soit, commis sur la personne d'un enfant qui n'a pas atteint l'âge de quatorze ans accomplis. Dans ce cas, la peine sera la réclusion de quinze à vingt ans.) (Elle sera de la réclusion de vingt ans à trente ans si l'enfant était âgé de moins de dix ans accomplis.)"

Art. 376. du Code pénal: "Si le viol ou l'attentat à la pudeur a causé la mort de la personne sur laquelle il a été commis, le coupable sera puni (de la réclusion de vingt ans à trente ans). (Si le viol ou l'attentat à la pudeur a été précédé ou accompagné des actes visés à l'article 417ter, alinéa premier, ou de séquestration, le coupable sera puni de la réclusion de quinze ans à vingt ans.) Si le viol ou l'attentat à la pudeur a été commis soit sur une personne [1 dont la situation de vulnérabilité en raison de l'âge, d'un état de grossesse, d'une maladie, d'une infirmité ou d'une déficience physique ou mentale était apparente ou connue de l'auteur des faits]1, soit sous la menace d'une arme ou d'un objet qui y ressemble, le coupable sera puni (de la réclusion) de dix à quinze ans."

Art. 377. du Code pénal: "[1 Les peines seront fixées comme prévu aux alinéas 2 à 6:
- si le coupable est l'ascendant ou l'adoptant de la victime, un descendant en ligne directe de la victime ou un descendant en ligne directe d'un frère ou d'une sœur de la victime; - si le coupable est soit le frère ou la sœur de la victime mineure ou toute personne qui occupe une position similaire au sein de la famille, soit toute personne cohabitant habituellement ou occasionnellement avec elle et qui a autorité sur elle; - si le coupable est de ceux qui ont autorité sur la victime; s'il a abusé de l'autorité ou des facilités que lui confèrent ses fonctions; s'il est médecin, chirurgien, accoucheur ou officier de santé et que l'enfant ou toute autre personne vulnérable visée à l'article 376, alinéa 3, fut confié à ses soins; - si dans le cas des articles 373, 375 et 376, le coupable, quel qu'il soit, a été aidé dans l'exécution du crime ou du délit, par une ou plusieurs personnes.]1 (Dans les cas prévus par le § 1 de l'article 372 et par le § 2 de l'article 373, la peine sera celle de la réclusion de dix ans à quinze ans.) (Dans le cas prévu par le paragraphe 1 de l'article 373, le minimum de l'emprisonnement sera doublé. (Dans les cas prévus par l'alinéa 3 de l'article 373, par l'alinéa 4 de l'article 375 et par l'alinéa 3 de l'article 376, la peine de la réclusion sera de douze ans au moins;) Dans le cas prévu par le paragraphe 1 de l'article 375, la peine de la réclusion sera de sept ans au moins. (Dans les cas prévus par les alinéas 5 et 6 de l'article 375 et par l'alinéa 2 de l'article 376, la peine de la réclusion sera de dix-sept ans au moins.)"

Art. 377bis. du Code pénal: "Dans les cas prévus par le présent chapitre, le minimum des peines portées par ces articles peut être doublé s'il s'agit d'un emprisonnement, et augmenté de deux ans s'il s'agit de la réclusion, lorsqu'un des mobiles du crime ou du délit est la haine, le mépris ou l'hostilité à l'égard d'une personne en raison de sa prétendue race, de sa couleur de peau, de son ascendance, de son origine nationale ou ethnique, de sa nationalité, de son sexe, de son orientation sexuelle, de son état civil, de sa naissance, de son âge, de sa fortune, de sa conviction religieuse ou philosophique, de son état de santé actuel ou futur, d'un handicap, de sa langue, de sa conviction politique, [1 de sa conviction syndicale,]1 d'une caractéristique physique ou génétique ou de son origine sociale."

Art. 377ter. du Code pénal: "[1 Dans les cas prévus par le présent chapitre ou par les chapitres VI et VII du présent titre, le minimum des peines portées par les articles concernés est doublé s'il s'agit d'un emprisonnement, et augmenté de deux ans s'il s'agit de la réclusion, lorsque le crime ou le délit a été commis à l'encontre d'un mineur de moins de seize ans accomplis et que préalablement à ce crime ou à ce délit, l'auteur avait sollicité ce mineur dans l'intention de commettre ultérieurement les faits visés au présent chapitre ou aux chapitres VI et VII du présent titre. Dans les cas visés à l'article 377, alinéas 4 à 6, l'augmentation du minimum de la peine prévue à l'alinéa 1er est limitée de telle sorte que, combinée à l'augmentation des peines prévue à l'article 377bis, elle n'excède pas le maximum de la peine prévu.]1"

Art. 377quater. du Code pénal "[1 La personne majeure qui, par le biais des technologies de l'information et de la communication, propose une rencontre à un mineur de moins de seize ans accomplis dans l'intention de commettre une infraction visée au présent chapitre ou aux chapitres VI et VII du présent titre, sera punie d'un emprisonnement d'un an à cinq ans, si cette proposition a été suivie d'actes matériels conduisant à ladite rencontre.]1"

Art. 378. du Code pénal: "Dans les cas prévus par le présent chapitre, les coupables seront condamnés à l'interdiction des droits énoncés à [1 l'article 31, alinéa 1er]1.

[2 Les tribunaux pourront en outre interdire au condamné, à terme ou à titre perpétuel, d'exploiter directement ou indirectement une maison de repos, un home, une seigneurie ou toute structure d'hébergement collectif de personnes visées à l'article 376, alinéa 3, ou de faire partie, comme membre bénévole, membre du personnel statutaire ou contractuel ou comme membre des organes d'administration et de gestion, de toute institution ou association dont l'activité concerne à titre principal des personnes vulnérables telles que visées à l'article 376, alinéa 3. L'application de cette interdiction se fera conformément à l'article 389.]"

Art. 378bis. du Code pénal: "La publication et la diffusion par le livre, la presse, la cinématographie, la radiophonie, la télévision ou par quelque autre manière, de textes, de dessins, de photographies, d'images quelconques ou de messages sonores de nature à révéler l'identité de la victime d'une infraction visée au présent chapitre sont interdites, sauf si cette dernière a donné son accord écrit ou si le procureur du Roi ou le magistrat chargé de l'instruction a donné son accord pour les besoins de l'information ou de l'instruction. Les infractions au présent article sont punies d'un emprisonnement de deux mois à deux ans et d'une amende de trois cents [euros] à trois mille [euros] ou d'une de ces peines seulement."

CHAPITRE VI. - (DE LA CORRUPTION DE LA JEUNESSE ET DE LA PROSTITUTION).

Art. 379. du Code pénal: "Quiconque aura attenté aux mœurs en excitant, favorisant ou facilitant, pour satisfaire les passions d'autrui, la débauche, la corruption ou la prostitution d'un mineur de l'un ou de l'autre sexe, sera puni de réclusion (de cinq ans à dix ans) et d'une amende de cinq cents [euros] à vingt-cinq mille [euros]. Il sera puni (de la réclusion) de dix ans à quinze ans et d'une amende de cinq cents [euros] à cinquante mille [euros] si le mineur n'a pas atteint l'âge de seize ans accomplis. (La peine sera de la réclusion de quinze ans à vingt ans et d'une amende de mille [euros] à cent mille [euros], si le mineur n'a pas atteint l'âge de quatorze ans accomplis.)"

Art. 380. du Code pénal: "§ 1. Sera puni d'un emprisonnement d'un an à cinq ans et d'une amende de cinq cents [euros] à vingt-cinq mille [euros]: 1° quiconque, pour satisfaire les passions d'autrui, aura embauché, entraîné, détourne ou retenu, en vue de la débauche ou de la prostitution, même de son consentement, une personne majeure (...); 2° quiconque aura tenu une maison de débauche ou de prostitution; 3° quiconque aura vendu, loué ou mis à disposition aux fins de la prostitution des chambres ou tout autre local dans le but de réaliser un profit anormal; 4° quiconque aura, de quelque manière que ce soit, exploité la débauche ou la prostitution d'autrui. § 2. La tentative de commettre les infractions visées au § 1er sera punie d'un emprisonnement de six mois à trois ans et d'une amende de cent [euros] à cinq mille [euros]. § 3. Seront punies (de la réclusion) de dix ans à quinze ans et d'une amende de cinq cents [euros] à cinquante mille [euros], les infractions visées au § 1er, dans la mesure où leur auteur: 1° fait usage, de façon directe ou indirecte, de manœuvres frauduleuses, de violence, de menaces ou d'une forme quelconque de contrainte; 2° ou abuse de la [1 situation de vulnérabilité dans laquelle se trouve une personne en raison de sa situation administrative illégale ou précaire, de son âge, d'un état de grossesse, d'une maladie, d'une infirmité ou d'une déficience physique ou mentale].

§ 4. Sera puni (de la réclusion) de dix ans à quinze ans et d'une amende de mille [euros] à cent mille [euros]: 1° quiconque, pour satisfaire les passions d'autrui, aura embauché, entraîné, détourné ou retenu, soit directement soit par un intermédiaire, un mineur (...), même de son consentement, en vue de la débauche ou de la prostitution; 2° quiconque aura tenu, soit directement soit par un intermédiaire, une maison de débauche ou de prostitution où des mineurs se livrent à la prostitution ou à la débauche;

3° quiconque aura vendu, loué ou mis à disposition d'un mineur, aux fins de la débauche ou de la prostitution, des chambres ou tout autre local dans le but de réaliser un profit anormal; 4° quiconque aura exploité, de quelque manière que ce soit, la débauche ou la prostitution d'un mineur (...).(5° quiconque aura obtenu par la remise, l'offre ou la promesse d'un avantage matériel ou financier, la débauche ou la prostitution d'un mineur.) § 5. (Les infractions visées au § 4 seront punies de la réclusion de quinze ans à vingt ans et d'une amende de mille [euros] à cent mille [euros] si elles sont commises à l'égard d'un mineur de moins de seize ans.) (§ 6. Quiconque aura assisté à la débauche ou à la prostitution d'un mineur sera puni d'un emprisonnement de un mois à deux ans et d'une amende de cent [euros] à deux mille [euros].) § 7. L'amende sera appliquée autant de fois qu'il y a de victimes.]".

Art. 380bis. du Code pénal: "Sera puni d'un emprisonnement de huit jours à trois mois et d'une amende de vingt-six [euros] à cinq cents [euros], quiconque, dans un lieu public aura par paroles, gestes ou signes provoqué une personne à la débauche. La peine sera élevée au double si le délit a été commis envers un mineur."

Art. 380ter. du Code pénal: "§ 1. Sera puni d'un emprisonnement de deux mois à deux ans et d'une amende de deux cents [euros] à deux mille [euros], quiconque, quel qu'en soit le moyen, fait ou fait faire, publie, distribue ou diffuse de la publicité, de façon directe ou indirecte, même en en dissimulant la nature sous des artifices de langage, pour une offre de services à caractère sexuel, lorsque cette publicité s'adresse spécifiquement à des mineurs ou lorsqu'elle fait état de services proposés soit par des mineurs, soit par des personnes prétendues telles. La peine sera d'un emprisonnement de trois mois à trois ans et d'une amende de trois cents [euros] à trois mille [euros] lorsque la publicité visée à l'article 1er a pour objet ou pour effet, directs ou indirects, de faciliter la prostitution ou la débauche d'un mineur ou son exploitation à des fins sexuelles.

§ 2. Sera puni d'un emprisonnement d'un mois à un an et d'une amende de cent [euros] à mille [euros], quiconque, quel qu'en soit le moyen, fait ou fait faire, publie, distribue ou diffuse de la publicité, de façon directe ou indirecte, même en en dissimulant la nature sous des artifices de langage, pour une offre de services à caractère sexuel, lorsque ces services sont fournis par un moyen de télécommunication. § 3. Dans les cas qui ne sont pas visés aux §§ 1er et 2, sera puni d'un emprisonnement d'un mois à un an et d'une amende de cent [euros] à mille [euros], quiconque aura, par un moyen quelconque de publicité, même en dissimulant la nature de son offre ou de sa demande sous des artifices de langage, fait connaître qu'il se livre à la prostitution, qu'il facilite la prostitution d'autrui ou qu'il désire entrer en relation avec une personne se livrant à la débauche. Sera puni des mêmes peines, quiconque, par un moyen quelconque de publicité, incitera, par l'allusion qui y est faite, à l'exploitation de mineurs ou de majeurs à des fins sexuelles, ou utilisera une telle publicité à l'occasion d'une offre de services."

Art. 381. du Code pénal: "Les infractions visées aux articles 379 et 380, §§ 3 et 4, seront punies de la réclusion de quinze ans à vingt ans et d'une amende de mille [euros] à cent mille [euros] et les infractions visées à l'article 380, § 5, seront punies de la réclusion de dix-sept ans à vingt ans et d'une amende de mille [euros] à cent mille [euros], si elles constituent des actes de participation à l'activité principale ou accessoire d'une association, et ce, que le coupable ait ou non la qualité de dirigeant."

Art. 382. du Code pénal: "§ 1er. Dans les cas visés aux articles 379 et 380, les coupables seront, en outre, condamnés à l'interdiction des droits énoncés à [1 l'article 31, alinéa 1er]1. § 2. Les tribunaux pourront interdire aux personnes condamnées pour une infraction prévue à l'article 380, §§ 1er à 3, pour un terme de un an à trois ans, d'exploiter, soit par eux-mêmes, soit par personne interposée, un débit de boissons, un bureau de placement, une entreprise de spectacles, une agence de location ou de vente de supports visuels, un hôtel, une agence de location de meublés, une agence de voyage, une entreprise de courtage matrimonial, une institution d'adoption, un établissement à qui l'on confie la garde des mineurs, une entreprise qui assure le transport d'élèves et de groupements de jeunesse, un établissement de loisirs ou de vacances, ou tout établissement proposant des soins corporels ou psychologiques, ou d'y être employés à quelque titre que ce soit.

En cas de seconde condamnation pour une infraction prévue à l'article 380, §§ 1er à 3, l'interdiction pourra être prononcée pour un terme de un an à vingt ans. En cas de condamnation pour une infraction prévue aux articles 379 et 380, §§ 4 et 5, l'interdiction pourra être prononcée pour un terme de un à vingt ans. § 3. Sans avoir égard à la qualité de la personne physique ou morale de l'exploitant, propriétaire, locataire ou gérant, le tribunal peut ordonner la fermeture de l'établissement dans lequel les infractions ont été commises, pour une durée d'un mois à trois ans.

Lorsque le condamné n'est ni propriétaire, ni exploitant, ni locataire, ni gérant de l'établissement, la fermeture ne peut être ordonnée que si la gravité des circonstances concrètes l'exige, et ce, pour une durée de deux ans au plus, après citation sur requête du ministère public, du propriétaire, de l'exploitant, du locataire ou du gérant de l'établissement. La citation devant le tribunal est transcrite à la conservation des hypothèques de la situation des biens à la diligence de l'huissier auteur de l'exploit. La citation doit contenir la désignation cadastrale de l'immeuble concerné et en identifier le propriétaire dans la forme et sous la sanction prévues à l'article 12 de la loi du 10 octobre 1913 portant des modifications à la loi hypothécaire et à la loi sur l'expropriation forcée et réglant à nouveau l'organisation de la conservation des hypothèques. Toute décision rendue en la cause est mentionnée en marge de la transcription de la citation selon la procédure prévue par l'article 84 de la loi hypothécaire. Le greffier fait parvenir au conservateur des hypothèques les extraits et la déclaration selon laquelle aucun recours n'est introduit. § 4. L'article 389 est applicable à la présente disposition."

Art. 382bis. du Code pénal: "Sans préjudice de l'application de l'article 382, toute condamnation pour des faits visés aux articles 372 à 377, [377quater,] 379 à 380ter, 381 et 383 à 387, accomplis sur un mineur ou impliquant sa participation, peut comporter, pour une durée d'un an à vingt ans, l'interdiction du droit: 1° de participer, à quelque titre que ce soit, à un enseignement donné dans un établissement public ou privé qui accueille des mineurs; 2° de faire partie, comme membre bénévole, membre du personnel statutaire ou contractuel, ou comme membre des organes d'administration et de gestion, de toute personne morale ou association de fait dont l'activité concerne à titre principal les mineurs;

3° d'être affecté à une activité qui place le condamné en relation de confiance ou d'autorité vis-à-vis de mineurs, comme membre bénévole, membre du personnel statutaire ou contractuel ou comme membre des organes d'administration et de gestion, de toute personne morale ou association de fait. [4° d'habiter, de résider ou de se tenir dans la zone déterminée désignée par le juge compétent. L'imposition de cette mesure doit être spécialement motivée et tenir compte de la gravité des faits et de la capacité de réinsertion du condamné.] L'article 389 est applicable à la présente disposition."

Art. 382ter. du Code pénal: "[La confiscation spéciale visée à l'article 42, 1°, est appliquée même si la propriété des choses sur lesquelles elle porte n'appartient pas au condamné, sans que cette confiscation puisse cependant porter préjudice aux droits des tiers sur les biens susceptibles de faire l'objet de la confiscation. Elle doit également être appliquée, dans les mêmes circonstances, au bien meuble, à la partie de celui-ci, au bien immeuble, à la chambre ou à tout autre espace. Elle peut également être appliquée à la contre-valeur de ces meubles ou immeubles aliénés entre la commission de l'infraction et la décision judiciaire définitive. En cas de saisie d'un bien immeuble, il est procédé conformément aux formalités de l'article 35bis du Code d'instruction criminelle.]"

Art. 382quater. du Code pénal: "[Lorsqu'un auteur qui est condamné pour des faits visés aux articles 372 à 377, [377quater,] 379 à 380ter et 381 est en contact, en raison de son état ou de sa profession, avec des mineurs et qu'un employeur, une personne morale ou une autorité qui exerce le pouvoir disciplinaire est connu, le juge peut ordonner la transmission de la partie pénale du dispositif de la décision judiciaire à cet employeur, cette personne morale ou ce pouvoir disciplinaire. Cette mesure est prise soit d'office, soit à la demande de la partie civile ou du ministère public dans une décision judiciaire spécialement motivée en raison de la gravité des faits, de la capacité de réinsertion ou du risque de récidive.]"

CHAPITRE VII. - DES OUTRAGES PUBLICS AUX BONNES MŒURS.

Art. 383. du Code pénal: "Quiconque aura exposé, vendu ou distribué des chansons, pamphlets ou autres écrits imprimés ou non, des figures ou des images contraires aux bonnes mœurs, sera condamné à un emprisonnement de huit jours à six mois et à une amende de vingt-six [euros] à cinq cents [euros]. (Sera puni des mêmes peines quiconque aura chanté, lu, récité, fait entendre ou proféré des obscénités dans les réunions ou lieux publics visés au § 2 de l'article 444.) (Sera puni des mêmes peines: Quiconque aura, en vue du commerce ou de la distribution, fabriqué, détenu, importe ou fait importer, transporte ou fait transporter, remis à un agent de transport ou de distribution, annoncé par un moyen quelconque de publicité, des chansons, pamphlets, écrits, figures ou images contraires aux bonnes mœurs;) Quiconque aura exposé, vendu ou distribué des emblèmes ou objets contraires aux bonnes mœurs, les aura, en vue du commerce ou de la distribution, fabriques ou détenus, importés ou fait importer, transportés ou fait transporter, remis à un agent de transport ou de distribution, annoncés par un moyen quelconque de publicité.) (Quiconque aura, soit par l'exposition, la vente ou la distribution d'écrits imprimés ou non, soit par tout autre moyen de publicité, préconisé l'emploi de moyens quelconques de faire avorter une femme, aura fourni des indications sur la manière de se les procurer ou de s'en servir ou aura fait connaître, dans le but de les recommander, les personnes qui les appliquent. Quiconque aura exposé, vendu, distribue, fabriqué ou fait fabriquer, fait importer, fait transporter, remis à un agent de transport ou de distribution, annoncé par un moyen quelconque de publicité les drogues ou engins spécialement destinés à faire avorter une femme ou annoncés comme tels.)"

Art. 383bis. du Code pénal: "§ 1. (Sans préjudice de l'application des articles 379 et 380, quiconque aura exposé, vendu, loué, distribué, diffusé ou remis des emblèmes, objets, films, photos, diapositives ou autres supports visuels qui représentent des positions ou des actes sexuels à caractère pornographique, impliquant ou présentant des mineurs ou les aura, en vue du commerce ou de la distribution, fabriqués ou détenus, importés ou fait importer, remis à un agent de transport ou de distribution, sera puni de la réclusion de cinq ans à dix ans et d'une amende de cinq cents [euros] à dix mille [euros].)

§ 2. Quiconque aura sciemment possédé les emblèmes, objets, films, photos, diapositives ou autres supports visuels visés sous le § 1er [1 ou y aura, en connaissance de cause, accédé par un système informatique ou par tout moyen technologique]1, sera puni d'un emprisonnement d'un mois à un an et d'une amende de cent [euros] à mille [euros]. § 3. L'infraction visée sous le § 1er, sera punie (de la réclusion) de dix ans à quinze ans et d'une amende de cinq cents [euros] à cinquante mille [euros], si elle constitue un acte de participation à l'activité principale ou accessoire d'une association, et ce, que le coupable ait ou non la qualité de dirigeant. § 4. La confiscation spéciale prévue à l'article 42, 1°, peut être appliquée à l'égard des infractions visées aux §§ 1er et 2, même lorsque la propriété des choses sur lesquelles elle porte n'appartient pas au condamné. § 5. (Les articles 382 et 389 sont applicables) aux infractions visées aux §§ 1er et 3."

Art. 384. du Code pénal: "art. 2 (Dans les cas visés à l'article 383), l'auteur de l'écrit, de la figure, de l'image ou de l'objet, sera puni d'un emprisonnement d'un mois à un an et d'une amende de cinquante [euros] à mille [euros]."

Art. 385. du Code pénal: "Quiconque aura publiquement outragé les mœurs par des actions qui blessent la pudeur, sera puni d'un emprisonnement de huit jours à un an et d'une amende de vingt-six [euros] à cinq cents [euros]. (Si l'outrage a été commis en présence d'un mineur âgé de moins de seize ans accomplis, la peine sera d'un emprisonnement d'un mois à trois ans et d'une amende de cent [euros] à mille [euros].)"

Art. 386. du Code pénal: "art. 2 Si les délits prévus à l'article 383 ont été commis envers des mineurs, l'emprisonnement sera de six mois à deux ans et l'amende de mille [euros] à cinq mille [euros]. Dans le même cas et sans préjudice de l'application de l'alinéa 2 de l'article 385, les peines prévues à l'alinéa premier de cet article pourront être portées au double."

Art. 387. du Code pénal: "Sera puni d'un emprisonnement de six mois à deux ans et d'une amende de mille [euros] à cinq mille [euros], quiconque vend ou distribue à des mineurs ou expose sur la voie publique ou le long de celle-ci des images, figures ou objets indécents de nature à troubler leur imagination."

Art. 388. du Code pénal: "Dans les cas prévus au présent chapitre, les coupables pourront de plus être condamnés à l'interdiction des droits énoncés à [l'article 31, alinéa 1er]. En cas de condamnation par application des articles 386, alinéa 1er, ou 387 et si l'infraction a été commise dans l'exploitation d'un commerce de librairie, de bouquinerie ou de produits photographiques ou de matériel nécessaire à la réalisation de tout type de support visuel, ou d'une entreprise de spectacles, la fermeture de l'établissement pourra être ordonnée pour une durée d'un mois à trois mois. En cas de deuxième condamnation du chef de l'un des faits visés à l'alinéa 2, commis dans le délai de trois ans à compter de la première condamnation, la fermeture pourra être ordonnée pour une durée de trois mois à six mois. En cas de troisième condamnation du chef des mêmes faits, commis dans le délai de cinq ans à dater de la deuxième condamnation, la fermeture définitive pourra être ordonnée.

Dans ce dernier cas, les cours et tribunaux pourront en outre interdire aux condamnés d'exploiter, soit par eux-mêmes, soit par personne interposée, une librairie, une bouquinerie, un commerce de produits photographiques ou de matériel nécessaire à la réalisation de tout type de support visuel, une entreprise de spectacles ou un ou plusieurs de ces commerces ou entreprises ou d'y être employés à quelque titre que ce soit. Lorsque le condamné n'est ni propriétaire, ni exploitant, ni locataire, ni gérant de l'établissement, la fermeture ne peut être ordonnée que si la gravité des circonstances concrètes l'exige. Dans ce cas, l'article 382, § 3, alinéas 2 à 5, est applicable. L'article 389 est applicable à la présente disposition."

Art. 389. du Code pénal: "§ 1er. La durée de l'interdiction prononcée en application des articles 378, 382, § 1er, 382bis et 388, alinéa 1er, courra du jour de la condamnation avec sursis ou du jour où le condamné aura subi ou prescrit sa peine d'emprisonnement non assortie du sursis et, en cas de libération anticipée, à partir du jour de sa mise en liberté pour autant que celle-ci ne soit pas révoquée. Toutefois, l'interdiction prononcée en application de l'article 382, § 2, produira ses effets à compter du jour où la condamnation contradictoire ou par défaut sera devenue irrévocable. § 2.

Toute infraction à la disposition du jugement ou de l'arrêt qui prononce une interdiction en application des articles visés au § 1er sera punie d'un emprisonnement d'un mois à six mois et d'une amende de cent [euros] à mille [euros] ou d'une de ces peines seulement. § 3. La fermeture prononcée en application des articles 382, § 3, et 388 produira ses effets à compter du jour où la condamnation contradictoire ou par défaut sera devenue irrévocable. § 4. Toute infraction à la disposition du jugement ou de l'arrêt qui ordonne la fermeture d'un établissement en application des articles visés au § 3 sera punie d'un emprisonnement de trois mois à trois ans et d'une amende de mille [euros] à cinq mille [euros] ou d'une de ces peines seulement."

Art. 433bis/1. "[Sera puni d'un emprisonnement de trois mois à cinq ans, la personne majeure qui communique par le biais des technologies de l'information et de la communication avec un mineur avéré ou supposé, et ce en vue de faciliter la perpétration à son égard d'un crime ou d'un délit: 1° s'il a dissimulé ou menti sur son identité ou son âge ou sa qualité; 2° s'il a insisté sur la discrétion à observer quant à leurs échanges; 3° s'il a offert ou fait miroiter un cadeau ou un avantage quelconque; 4° s'il a usé de toute autre manœuvre.]"

Art. 210bis du Code pénal: "§ 1er. 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, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de vingt-six [euros] à cent mille [euros] ou d'une de ces peines seulement. § 2. Celui qui fait usage des données ainsi obtenues, tout en sachant que celles-ci sont fausses, est puni comme s'il était l'auteur du faux. § 3. La tentative de commettre l'infraction visée au § 1er et est punie d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six [euros] à cinquante mille [euros] ou d'une de ces peines seulement. § 4. Les peines prévues par les §§ 1er à 3 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans qui suivent le prononcé d'une condamnation pour une de ces infractions ou pour une des infractions prévues aux articles 259bis, 314bis, 504quater ou au titre IX bis".

Art. 504quater du Code pénal: "§1er. (Celui qui cherche à se procurer, pour lui-même ou pour autrui, avec une 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, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de vingt-six [euros] à cent mille [euros] ou d'une de ces peines seulement. § 2. La tentative de commettre l'infraction visée au § 1er et est punie d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six [euros] à cinquante mille [euros] ou d'une de ces peines seulement. § 3. Les peines prévues par les §§ 1er et 2 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans qui suivent le prononcé d'une condamnation pour une de ces infractions ou pour une des infractions visées aux articles 210bis, 259bis, 314bis ou au titre IX bis".