Conseil de
l'Union européenne

Bruxelles, le 19 mai 2017
(OR. fr)

7162/1/17
REV 1 DCL 1

GENVAL 22
CYBER 38

DÉCLASSIFICATION

du document:	7162/1/17 REV 1 RESTREINT UE/EU RESTRICTED
en date du:	2 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 le Luxembourg

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 2 mai 2017
(OR. fr)

7162/1/17
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 22
CYBER 38

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 le Luxembourg

ANNEXE

SOMMAIRE

1 RÉSUMÉ

- La mission d'évaluation au Luxembourg s'est déroulée dans un climat positif, les autorités luxembourgeoises ayant soigneusement préparé le programme ainsi que les entretiens de l'équipe d'évaluation avec les représentants des institutions et des ministères concernés.

- Pour ce qui est de la législation, le Luxembourg a transcrit dans son droit interne les principaux textes européens et internationaux traitant de la lutte contre la cybercriminalité, et il poursuit sa réflexion visant à améliorer son droit positif à travers différents projets de loi.

- La proximité des institutions et des partenaires externes en matière de cybersécurité fait du Luxembourg un État qui peut être cité en exemple pour son partenariat public-privé, notamment en termes de formation, sensibilisation et prévention, ainsi que pour son partage de savoir-faire, y compris au niveau international.

- Cependant, compte tenu de la multiplicité des approches, la capacité de réaction opérationnelle peut être améliorée, y compris au niveau international. Cette amélioration peut se traduire par un renforcement des ressources humaines et financières allouées aux différents acteurs, principalement au sein du Ministère de l'Intérieur.

2 INTRODUCTION

À la suite de l'adoption de l'action commune 97/827/JAI du 5 décembre 1997[1], 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 de cette action commune, le groupe "Questions générales, y compris l'évaluation" (GENVAL) a décidé, lors de sa 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 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[2] (date de transposition: 18 décembre 2013) et la directive 2013/40/UE relative aux attaques contre les systèmes d'information[3] (date de transposition: 4 septembre 2015) revêtent une importance particulière dans ce contexte.

1 Action commune 97/827/JAI du 5 décembre 1997 (JO L 344 du 15.12.1997, p. 7).
2 JO L 335 du 17.12.2011, p. 1.
3 JO L 218 du 14.8.2013, p. 8.

En outre, dans ses conclusions de juin 2013 relatives à la stratégie de cybersécurité de l'UE[4], 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)[5] et souligne, dans le préambule de ces mêmes conclusions, 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[6].

L'expérience des évaluations précédentes montre que la mise en œuvre des instruments juridiques concernés se situe 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, l'évaluation 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.

4 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.

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

6 STE nº 189, ouvert à la signature le 28 janvier 2003 et entré 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. Le Luxembourg est le vingt-cinquième État membre évalué au cours de cette série d'évaluations. Conformément à l'article 3 de l'action commune susmentionnée, 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 composent 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 du Luxembourg étaient Monsieur Yves Vandermeer et Monsieur Stephane Robinot, ainsi que Madame Carmen Necula, du Secrétariat Général du Conseil.

Le présent rapport a été élaboré par l'équipe d'experts précités, avec l'assistance du Secrétariat général du Conseil, sur la base des constatations émises à la suite de la visite d'évaluation effectuée au Luxembourg du 6 au 9 juin 2016 et des réponses détaillées du Luxembourg au questionnaire d'évaluation, accompagnées de ses réponses détaillées aux questions complémentaires qui lui ont ensuite été adressées.

3 QUESTIONS GÉNÉRALES ET STRUCTURES

3.1 Stratégie nationale en matière de cybersécurité

Le Luxembourg dispose d'une stratégie de cybersécurité. La version anglaise peut être téléchargée sur le site de l'ENISA: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf

Cette stratégie vise aussi à lutter contre la cybercriminalité. Des actions générales, mais aussi des actions concrètes, sont proposées:

- Actions générales: le Luxembourg favorise la collaboration nationale et internationale. En effet, la cybersécurité n'est pas un défi individuel, mais bien collectif. Le Luxembourg favorise la collaboration et l'échange par la création d'une taxonomie commune basée sur l'approche "risques". Cette approche coordonnée réduit l'effort individuel, ainsi que la complexité que chaque entité doit affronter, et démocratise ainsi la cybersécurité.
- Actions spécifiques: le Luxembourg a aussi prévu des actions spécifiques pour rendre la lutte contre la cybercriminalité plus efficace. Parmi celles-ci figurent notamment les groupes d'échange et de coordination entre le parquet, les services de police et le CERT, la coopération avec Europol, l'EUCTF, Interpol et le FBI, l'ICCAM comme plateforme d'échange avec Interpol et les lignes directes (hotlines) INHOPE.

3.2 Priorités nationales en matière de cybercriminalité

- Prévention

Le Luxembourg est conscient que la prévention joue un rôle fondamental dans la lutte contre la cybercriminalité. C'est pour cette raison qu'il investit beaucoup d'efforts afin de sensibiliser toutes les personnes concernées (jeunes, adultes, personnes âgées, employés privés et fonctionnaires). Citons à cet égard les grands "programmes" grâce auxquels le Luxembourg sensibilise les différents publics cibles: BEE SECURE pour les personnes individuelles (enfants, jeunes, parents et encadrants, adultes au sens large et seniors) et CASES pour les administrations publiques et les entreprises privées. Le Luxembourg met aussi à la disposition de tous des méthodes pour améliorer la sécurité organisationnelle, notamment les outils comme MONARC (Méthode optimisée d'analyse des risques CASES) ainsi qu'un diagnostic sécurité.

- Formation

La sensibilisation aux risques liés à la société numérique, et donc aussi à la cybercriminalité, est obligatoire dans l'enseignement secondaire pour toutes les classes de 7^{e} ainsi que pour tous les jeunes fonctionnaires. La sensibilisation obligatoire dans l'enseignement fondamental est en cours d'élaboration, mais elle est déjà actuellement pratiquée à une grande échelle. Des formations sont proposées au secteur privé à des tarifs intéressants (25 €/personne). BEE SECURE offre des séances d'information et des formations pour parents, enseignants et éducateurs sur demande. Ces actions de sensibilisation et de formation fournissent beaucoup d'informations sur les menaces liées à la cybercriminalité.

- Détection

Le Luxembourg a reconnu qu'il est primordial de détecter aussi vite que possible les cas de compromission de systèmes informatiques et de réagir efficacement. Par conséquent, le Luxembourg dispose de quatre CERT publics et de sept CERT privés. Les CERT échangent entre eux des informations sur les indicateurs de compromission via la plateforme d'échange MISP. Un grand nombre d'entreprises (qui doivent avoir un certain degré d'importance) sont aussi connectées à cette plateforme d'échange.

- Réponse sur incidents

Le Luxembourg dispose de quatre CERT publics qui gèrent proactivement les incidents en relation avec le Luxembourg. Le Luxembourg est très conscient de l'importance de réagir vite et efficacement. Le projet BGP Ranking documente d'ailleurs de façon très détaillée l'efficacité des CERT luxembourgeois.

- Coopération internationale

Le Luxembourg est très actif à plusieurs niveaux:

- les CERT luxembourgeois sont fortement connectés
- le Luxembourg est très actif au niveau de l'ENISA
- le KannerJugendTelefon en tant qu'opérateur de la BEE SECURE Stopline est membre de INHOPE – International Association of Internet Hotlines. Le Luxembourg est aussi membre actif du réseau Insafe ("Safer Internet Centres" à travers l'Europe) via l'initiative BEE SECURE.

- BEE SECURE – sensibilisation du grand public, opéré par le Service National de la Jeunesse, Securitymadein.lu et le "KannerJugendTelefon" (numéro d'appel gratuit de type "helpline" destiné aux enfants et aux jeunes). BEE SECURE est une initiative commune du Ministère de l'Economie, du Ministère de la Famille, de l'Intégration et à la Grande Région et du Ministère de l'Education nationale, de l'enfance et de la jeunesse.

3.3 Statistiques sur la cybercriminalité

3.3.1 Grandes tendances de la cybercriminalité

Tout d'abord, il convient de préciser que depuis le 1er avril 2011, le Parquet de Luxembourg dispose d'une section spécialisée en matière de cybercriminalité.

Une première statistique établie concernant les dossiers inscrits sous la référence "cyber" entre le 1er avril 2011 et le 1er décembre 2012 fait état de 385 dossiers sur une année et demie, et 228 pour la deuxième année. Entre 2013 et 2014, le nombre de dossiers inscrits sous cette référence a connu une progression de 50 % par rapport à l'année précédente (350 dossiers).

Entre le 1er janvier 2015 et le 31 décembre 2015, 470 dossiers "cyber" ont été inscrits, soit une nouvelle progression de près de 35 %.

Les escroqueries en tous genres (126) ont encore dépassé en nombre les extorsions et tentatives d'extorsion à l'aide de vidéos indélicates enregistrées à l'insu des victimes (99).
Parmi les principaux modes opératoires d'escroquerie, il y a lieu de signaler:

- location d'appartements inexistants (41)
- Microsoft Scam (26)
- ventes diverses par Internet d'objets inexistants (28)
- vente de chiens inexistants (9)
- vente de voitures inexistantes (8)
- location de vacances inexistantes (5)
- faux comptes Paypal (5)
- faux crédits (2)
- escroquerie dite "nigérienne" (2)

Les dossiers de "phishing" se sont stabilisés à 21 (contre 17 en 2013 et 35 en 2014).

Il y a lieu de noter la très nette augmentation (31 dossiers, contre 16 en 2014) des faux ordres de virement, c'est-à-dire des courriels envoyés par des criminels au nom d'un client d'une banque et demandant qu'un virement soit effectué au bénéfice d'un compte tiers (money mule) qui n'a aucun droit d'obtenir le montant concerné.

Un autre phénomène s'est développé au cours des années 2014 (30 dossiers) et 2015 (35 dossiers), à savoir les fraudes au président (CEO fraud). Dans ce type de fraude, l'auteur contacte le service comptable d'une entreprise, en se faisant passer pour le PDG ou un membre de la direction de celle-ci. Tout en insistant sur le caractère confidentiel de l'entretien, il donne des explications sur un important contrat qui devrait être conclu dans la plus grande urgence. L'auteur est généralement très bien informé sur la structure de l'entreprise visée et se sert de nombreuses pièces falsifiées préparées à l'avance pour justifier de la réalité et du sérieux de l'opération. Pièces à l'appui, il arrive à convaincre le comptable d'exécuter un virement en faveur d'un compte à l'étranger (généralement tenu par un money mule).

Sur les 470 dossiers, 370 ont dû être classés "auteur inconnu" et 27 ont été classés sans suite (en partie après une instruction judiciaire ou une enquête policière).

Dans 42 dossiers une enquête de police a été engagée ou poursuivie, dans onze dossiers une instruction judiciaire a été ouverte et dans six dossiers une mini-instruction a été demandée. Les éventuelles condamnations n'ont pas été répertoriées, le système informatique ne permettant pas de les différencier des autres condamnations. Il est néanmoins prévu que ce chiffre soit disponible pour les statistiques de 2016.

Les 470 dossiers ont entraîné un préjudice d'un montant d'au moins 3 052 315,37 euros (contre 2 108 764,07 euros en 2014). Il s'agit uniquement des pertes financières directement chiffrables. Cette nouvelle progression considérable est surtout liée aux dossiers "CEO fraud" et aux faux ordres de virement.

Comme tous les ans, il y a lieu de noter que les dossiers de vol à l'aide de données de cartes de crédit piratées, compte tenu de leur nombre impressionnant (3 ou 4 dossiers par jour, soit plus de 900 par an) et de l'absence d'identification d'e l'auteur, ne sont pas repris dans cette statistique, mais sont transmis de manière généralisée au SPJ section Criminalité générale aux fins de la centralisation et du traitement des informations recueillies au sein d'Europol en vue d'une enquête d'envergure à ce sujet.

En ce qui concerne les dossiers de pédopornographie, durant l'année 2013, 21 nouvelles affaires pour détention de matériel pédopornographique (article 384 du CP) et transmission de matériel pédopornographique (articles 383 et suivants du CP) ont été ouvertes. Sept dossiers ont été instruits pendant cette période et ont abouti à des jugements/arrêts de condamnation, tandis que deux dossiers ont donné lieu à un acquittement.

Pendant l'année 2014, 41 nouvelles affaires pour détention de matériel pédopornographique (article 384 du CP) et transmission de matériel pédopornographique (articles 383 et suivants du CP) ont été ouvertes. Treize dossiers ont été instruits pendant cette période et ont abouti à des jugements/arrêts de condamnation.

Enfin, en ce qui concerne l'année 2015, 29 nouvelles affaires pour détention de matériel pédopornographique (article 384 du CP) et transmission de matériel pédopornographique (articles 383 et suivants du CP) ont été ouvertes. Dix-neuf dossiers ont été instruits pendant cette période et ont abouti à des jugements/arrêts de condamnation.

Il est difficile de se prononcer sur le pourcentage de dossiers de cybercriminalité par rapport aux dossiers de droit commun. En tout état de cause, en 2015, 52 959 dossiers ont été enregistrés au Parquet de Luxembourg.

3.3.2 Nombre de cas de cybercriminalité répertoriés

Le service des statistiques judiciaires est compétent pour l'établissement de toutes les statistiques concernant les juridictions luxembourgeoises.

La Police Grand-Ducale n'a pas recours à des statistiques d'institutions externes et utilise uniquement des renseignements issus d'une base de données interne.

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

La prévention de la cybercriminalité est une des missions principales du GOVCERT, ce budget mis à disposition par l'État est investi entièrement dans ce domaine. Cependant, il faut savoir que ce budget est divisé en deux: une partie est utilisée à des fins d'acquisition de matériel (serveurs, PC, etc.) (60 000 € en 2015) et l'autre article budgétaire, utilisé pour assurer le bon fonctionnement du GOVCERT (consultance, études, ...), est limité à 530 000 €.

Le GOVCERT dispose des deux seuls articles budgétaires dédiés à la cybercriminalité:
- 30.6.74.310 – Computer Emergency Response Team (GOVCERT): acquisition et installation d'équipements spéciaux.
- 00.6.12.385 – Computer Emergency Response team (GOVCERT): frais de fonctionnement."

Le GOVCERT ne bénéficie pas d'un financement de l'UE pour assurer ses missions.
BEE SECURE dispose également d'un budget dans le cadre du programme "Connecting Europe Facility" de la Commission Européenne.

3.5 Conclusions

La nouvelle stratégie nationale en matière de cybersécurité, qui a été adoptée le 27 mars 2015, remplace et développe la version de 2013.

Après avoir défini les différentes notions liées à la cybersécurité (celles-ci faisaient défaut dans la stratégie de 2013), ce nouveau document fixe sept objectifs, accompagnés de leurs plans d'action respectifs. Les priorités en matière de cybersécurité sont: la prévention, la formation, la détection, la réponse sur incidents, la coopération internationale, la sensibilisation du public, ainsi que la sensibilisation et la formation des entités publiques et privées.

Force est de constater que le maître mot de cette stratégie est le renforcement de la coopération. Que ce soit au niveau national, international ou avec le monde académique, le Luxembourg possède d'ores et déjà, presque naturellement et culturellement, une solide base de coopération entre les différents acteurs nationaux.

Il doit néanmoins développer clairement son implication dans la coopération internationale, que ce soit dans le domaine de la cybercriminalité ou de la cybersécurité d'une manière plus large.
Pour autant, si la création de l'Agence nationale de la sécurité des systèmes d'information est à saluer, cette dernière n'est pas encore dotée des ressources humaines et techniques suffisantes pour l'accomplissement de ses missions. Bien que l'approche s'inscrive dans une collaboration future, à partir de 2017, avec d'autres entités, un minimum de moyens humains doivent pouvoir être dédiés au niveau de l'organe central.

Il existe, en matière de répression, un groupe de travail "cybercrime" regroupant les autorités nationales (parquet, police et CERT) aux fins d'échange d'informations régulières. Les sujets de discussion visent des sujets comme la coopération policière et/ou judiciaire aves les fournisseurs de services et la procédure de coopération/intervention entre police et les CERTs.

Du côté du Ministère de la Justice, les priorités nationales en matière de cybercriminalité apparaissent bien définies et identifient clairement les acteurs et la spécialisation des autorités judiciaires est une bonne pratique.

Les statistiques incluent des infractions purement informatiques et des infractions commises par l'intermédiaire d'un ordinateur, toutes reprises sous l'appellation "cyber". À l'instar de beaucoup d'autres pays européens, les autorités nationales reconnaissent l'existence d'un chiffre noir, c'est-à-dire les cas où la victime ne dépose pas plainte.

On constate que parmi les 470 dossiers "cyber" enregistrés en 2015, et bien que le préjudice ait été très élevé, un très grand nombre (370) ont été classés comme étant commis par un auteur inconnu. Les causes mentionnées par les autorités nationales sont l'impossibilité d'identifier les auteurs, la nature internationale de ce type d'infractions et les difficultés en matière de coopération et d'entraide judiciaire. Un autre obstacle mentionné est le fait que les ISP ne coopèrent pas et que les données ne se trouvent pas au Luxembourg.

Au Luxembourg, il y a onze CERT, dont quatre sont financés par le gouvernement. Le GOVCERT s'occupe des infrastructures critiques et travaille avec les services IT de chaque entité. C'est le point de contact unique pour les entités d'État. Sa principale tâche est le traitement d'incidents dans des infrastructures classifiées et non classifiées. Le directeur du GOVCERT préside la cellule d'évaluation du risque cyber. D'autres services offerts par GOVCERT sont: incident handling, détection des systèmes compromis, black listing, analyse de malware (automatique et manuelle), annonces et recommandations de sécurité.

D'autres CERT sont dédiés au domaine privé, au domaine de la santé ou au domaine de la recherche. Ces CERT ont des réunions tous les trois mois pour coordonner leurs politiques en matière de cybercriminalité.

En matière de prévention pour préparer et gérer de manière efficace une éventuelle crise, les autorités compétentes organisent des exercices et rédigent des plans pour assurer la coordination.

4 STRUCTURES NATIONALES

4.1 Système judiciaire (poursuites et juridictions)

4.1.1 Structure interne

Les institutions publiques responsables de la prévention de la cybercriminalité et de la lutte contre celle-ci

- BEE SECURE – sensibilisation du grand public, opéré par le Service national de la jeunesse, Securitymadein.lu et le "KannerJugendTelefon".
  - o Sensibilisation
  - o Assistance aux citoyens (BEE SECURE Helpline helpline.bee-secure.lu)
  - o Traitement de notifications anonymes (BEE SECURE Stopline stopline.bee-secure.lu) concernant les images d'abus sexuels sur mineur, les contenus racistes, révisionnistes ou discriminatoires et les contenus terroristes
- Cyber Security Board - organe centralisateur en matiere de lutte contre la cybercriminalité et également en matière de prévention
- CASES – sensibilisation – formation et sécurité organisationnelle pour les entités publiques et privées; opérée par securitymadein.lu
  - o Sensibilisation
  - o Formation
  - o Prévention au moyen de mesures organisationnelles
  - o Méthodes d'analyse des risques
- CIRCL, GovCERT – CERT publics
  - o Détection
  - o Réponse sur incident
- ANSSI (Agence nationale de la sécurité des systèmes d'information)
  - o Politiques de sécurité au niveau des acteurs publics ainsi que des opérateurs d'infrastructures critiques

Depuis le 1er avril 2011, le Parquet de Luxembourg dispose d'une section spécialisée en matière de cybercriminalité.

Actuellement, deux magistrats du parquet (un premier substitut et un substitut) et un magistrat au niveau de la Cellule de Renseignement Financier (premier substitut) s'occupent, entre autres (c'est-à-dire non exclusivement) des dossiers de cybercriminalité.

Cela ne comprend pas les dossiers de pédopornographie, qui sont traités par trois magistrats du parquet jeunesse (trois premiers substituts), de racisme, qui sont traités par un magistrat (substitut principal), et de terrorisme, qui sont traités par un autre magistrat (procureur d'État adjoint).

Au niveau du cabinet d'instruction, un juge d'instruction s'occupe plus spécifiquement des affaires de cybercriminalité.

4.1.2 Capacités disponibles et obstacles à l'aboutissement des poursuites

En matière de collecte de données informatiques par les autorités de poursuite, le Luxembourg a transposé le système instauré par la Convention de Budapest, qui prévoit une procédure en deux étapes: la première étape consiste à conserver des données pendant une certaine période et la deuxième permet de saisir ces données selon les procédures de droit commun.

Dans un souci de lisibilité des textes nationaux, le législateur luxembourgeois a défini une procédure générale de conservation des données, qui s'applique à toutes ces hypothèses. L'article 48-25 du CIC prévoit ainsi que:

"Lorsqu'il y a des raisons de penser que des données stockées, traitées ou transmises dans un système de traitement ou de transmission automatisé de données, utiles à la manifestation de la vérité, sont susceptibles de perte ou de modification, le procureur d'État ou le juge d'instruction saisi peut faire procéder à la conservation rapide et immédiate, pendant un délai qui ne peut excéder 90 jours, de ces données".

L'article 48-25 du CIC permet la conservation rapide de données dans le cadre du flagrant délit ou de l'enquête préliminaire par le procureur d'État et dans le cadre de l'instruction par le juge d'instruction. La procédure pourra être utilisée aussi bien au niveau national qu'au niveau international dans le cadre de commissions rogatoires internationales.

En pratique, le procureur d'État ou le juge d'instruction demandera, directement ou par l'intermédiaire de la police, au détenteur des données (notamment un hébergeur) de conserver celles-ci pendant un délai de 90 jours. Les magistrats pourront formuler cette demande dans le cadre d'un dossier national ou à la suite d'une demande d'une autorité compétente étrangère.

Ce n'est que dans une deuxième étape, qui ne saurait intervenir après un délai de 90 jours après la demande de conservation, que les données sont saisies dans le cadre d'une procédure nationale ou internationale.

Par ailleurs, le texte sur l'infiltration (article 48-17 du CIC) a également été complété pour les infractions en matière informatique au sens des articles 509-1 à 509-7 du CP. D'après le point 3 de l'article 48-17, "l'infiltration consiste à surveiller des personnes à l'encontre desquelles il existe des indices graves qu'elles commettent un ou plusieurs des faits visés au paragraphe précédent, en se faisant passer, auprès de ces personnes, notamment comme un de leurs coauteurs, complices ou receleurs".

La législation nationale sur l'infiltration est basée sur la législation française en la matière, telle qu'elle résulte des articles 706-81 à 706-87 du code de procédure pénale.

Le procureur d'État et le juge d'instruction peuvent désormais, dans des conditions posées par la loi, ordonner l'effacement de données, à condition que la détention ou l'usage de ces données soit illégal ou dangereux pour la sécurité des personnes ou des biens.

Les principaux obstacles à l'aboutissement de poursuites contre les actes de cybercriminalité sont les suivants:

- les instruments d'entraide judiciaire internationale sont trop lents et insuffisants pour faire face à la volatilité des preuves sur Internet,
- la durée, la diversité de la durée, voire l'absence totale de rétention des données d'un État à l'autre. Dans certains cas, les données de communication sont les seules données disponibles pour identifier le suspect,
- le chiffrement,
- les moyens rendant plus difficile, c'est-à-dire les moyens empêchant l'identification du suspect (réseaux peer-to-peer, TOR, DARKNET)
- les nouveaux moyens de paiement (bitcoin et systèmes dérivés) permettent aux criminels d'échapper plus facilement aux autorités et de dissimuler les transactions. Ces mécanismes de paiement sont complexes et de ce fait méconnus,
- la masse de données à analyser.

4.2 Autorités répressives

La structure des autorités répressives compétentes en matière de prévention de la cybercriminalité et de lutte contre celle-ci est la suivante:

- Le Parquet général (entraide judiciaire)
- Le Ministère public (enquête et poursuites)
- Le Cabinet d'instruction (instruction et mesures coercitives)
- La Cellule de renseignement financier (criminalité financière au moyen des nouvelles technologies)
- Les juridictions répressives

Le concept judiciaire (ligne directrice à tous les acteurs en matière judiciaire ayant été élaborée en concertation étroite avec l'autorité judiciaire) fixe la répartition des compétences et des missions entre les différents services de la Police Grand-Ducale en matière de police judiciaire.

En matière de lutte contre la cybercriminalité, les infractions dont l'objet est constitué par les technologies numériques (articles 509-1 à 509-7 du CP, piratage, intrusion, DDOS etc.) sont de la compétence exclusive de la section Nouvelles technologies du service de police judiciaire.
Dans toutes les autres infractions qui utilisent les technologies numériques (escroqueries, diffusion de contenus illicites, contrefaçon), le principe de subsidiarité détermine l'unité compétente. L'appui technique est assuré par les spécialistes de la section Nouvelles technologies.

Le seul moyen de combattre certains phénomènes néfastes (spamming, phishing, etc.) de l'internet est la prévention. La section Nouvelles technologies n'a pas pour première mission de s'occuper du domaine de la prévention et ne dispose pas de ressources pour ce faire, ce qui ne prête néanmoins pas à conséquence puisque cette tâche est reprise par d'autres structures, telles que BEE SECURE pour les personnes individuelles ou encore CASES pour les administrations publiques et les entreprises privées, cela en étroite collaboration avec les différents acteurs.

Le Service de police judiciaire, section Nouvelles technologies, est chargé des enquêtes en matière de cybercriminalité, à l'exception des dossiers de pédopornographie (SPJ, protection de la jeunesse), de terrorisme (SPJ, cellule anti-terrorisme) et des "CEO frauds" (SPJ, sections criminalité générale et anti-blanchiment, ainsi que la SREC de Grevenmacher).

Il n'y a pas de postes spéciaux prévus, les enquêteurs de la section Nouvelles technologies disposant d'une expertise et de connaissances spécifiques en matière informatique.

Lorsqu'il s'agit d'un cas de cybercriminalité grave, la section Nouvelles technologies dispose de trois enquêteurs spécialisés dans ce domaine. À leur demande, ils peuvent être assistés d'un ou plusieurs spécialistes IT-Forensic.

Ces spécialistes en informatique (ingénieur en informatique, télécommunication et électronique) sont recrutés depuis 2003 dans le civil. Ils reçoivent une formation d'officier de police judiciaire sanctionnée par un examen.

Les poursuites contre les actes de cybercriminalité sont longues et nécessitent le plus souvent des coopérations internationales et des commissions rogatoires.

Le Luxembourg a mis en place un point de contact disponible 24 heures sur 24 et 7 jours sur 7, assuré par un rôle de permanence opérationnelle au sein de la section Nouvelles technologies du SPJ.

4.3 Autres services et partenariat public-privé

CERT.LU est un exemple phare du partenariat public-privé des CERT au Luxembourg. Onze entités en font patie, quatre du secteur public et sept du secteur privé.

Les campagnes BEE SECURE, qui sont proposées à un rythme annuel, bénéficient d'un soutien large du secteur privé en ce qui concerne la diffusion des messages.

4.4 Coopération et coordination au niveau national

4.4.1 Obligations légales ou de principe

En matière de protection des données, l'article 3, paragraphe 3, de la loi modifiée du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques prévoit qu'"en cas de violation de données à caractère personnel, le fournisseur de services de communications électroniques accessibles au public avertit sans retard la Commission nationale pour la protection des données de la violation".

D'une façon générale, l'article 23, deuxième alinéa, du CIC oblige tout fonctionnaire qui acquiert la connaissance de faits susceptibles de constituer un crime ou un délit d'en donner avis sans délai au procureur d'État.

Dans le cadre du paquet télécom, les opérateurs doivent signaler les infractions au régulateur ILR.

Le Luxembourg dispose d'un mécanisme de coordination pluridisciplinaire afin de répondre à des cyberattaques importantes. Le Haut Commissariat à la Protection Nationale coordonne la réponse à de telles attaques. Il dispose aussi d'une cellule d'évaluation de la menace, appelée CERC (Cellule d'évaluation des risques cyber).

- http://www.infocrise.public.lu/fr/cyberattaque/index.html

Le plan d'intervention d'urgence "PIU Cyber", approuvé et rendu exécutoire par le Conseil de Gouvernement le 19 mars 2014, définit l'action du gouvernement en cas de faille technique ou d'attaque d'envergure contre les systèmes d'information du secteur public et/ou du secteur privé.

Les organes de gestion de crise sont le Single Point of Contact Cyber (SPOC Cyber), la Cellule d'évaluation du risque cyber (CERC) et la Cellule de crise Cyber.

- le "Single Point of Contact Cyber (SPOC Cyber)": point de contact unique, il fonctionne 24 heures sur 24 et 7 jours sur 7 afin de donner la possibilité aux acteurs nationaux et internationaux de signaler à tout moment aux autorités nationales les incidents majeurs dans le domaine cyber.
- la Cellule d'évaluation du risque cyber (CERC): composée d'experts, la CERC évalue l'évolution de la situation en cas de menace et met en place une veille renforcée en amont de l'activation éventuelle de la CC.
- la Cellule de crise Cyber (CC): elle est activée par le Premier ministre, ministre d'État, en cas d'imminence ou de survenance d'une crise. La CC initie, coordonne et veille à l'exécution de toutes les mesures destinées à faire face à une crise et à ses effets, y compris favoriser le retour à l'état normal. Elle prépare les décisions qui s'imposent et les soumet au gouvernement aux fins d'approbation. En cas d'intervention opérationnelle sur le terrain, sa mission s'étend à la coordination et au contrôle de l'exécution.

Le plan est déclenché lorsqu'un incident ou une attaque cyber sont signalés au SPOC Cyber par des administrations nationales ou par des acteurs internationaux. La SPOC Cyber alerte immédiatement la Cellule d'évaluation du risque cyber (CERC), qui procède à une évaluation des informations disponibles. Si l'incident est de nature à engendrer un impact significatif, le Haut-Commissaire à la protection nationale est alerté et en informe le Premier ministre, ministre d'État, qui décide de l'opportunité d'activer la CC. Celle-ci initie, coordonne et veille à l'exécution de toutes les mesures prévues pour faire face à la crise et rétablir le retour à la normale. Les mesures prévues sont les mesures d'évaluation, de veille renforcée, d'analyse technique, de cloisonnement, de mise à niveau et protection des systèmes et d'activation de la réserve nationale cyber et le rétablissement des services.

Les banques, de même que les établissements de paiement et de monnaie électronique, doivent respecter les dispositions édictées par la loi du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme portant transposition de la directive 2001/97/CE du Parlement européen et du Conseil du 4 décembre 2001 modifiant la directive 91/308/CEE du Conseil relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux (ci-après la "loi LB/FT").

La Cellule de Renseignement procède à de nombreux échanges internationaux en cette matière, afin de faire parvenir les informations concluantes à l'État membre concerné le plus rapidement possible.

- accroître la sécurité des paiements autres qu'en espèces et réduire la vulnérabilité des bandes magnétiques

Les établissements de paiement et de monnaie électronique doivent appliquer les mesures de vigilance imposées par la loi LB/FT. L'analyse des transactions effectuée par la cellule de renseignement financier a révélé que dans de très nombreux cas, les transactions frauduleuses sont bloquées avant que le gain escompté par le criminel ne lui ait été reversé.

- renforcer les procédures d'autorisation des transactions en ligne et l'authentification des clients

Mise en place du système "3D secure", aussi connu sous les appellations commerciales "Verified By Visa" et "MasterCard SecureCode".

La sécurisation des données électroniques et des transactions effectuées en ligne a également été renforcée par l'entrée en vigueur de la loi sur le commerce électronique, le 14 août 2000, et le règlement grand-ducal portant sur la signature électronique, qui définit les caractéristiques que celle-ci doit revêtir pour être reconnue comme légale (1er juin 2001).

Avec la création de LuxTrust S.A., dont deux tiers du capital sont détenus par l'État, une solution de sécurisation électronique commune a été mise en place, solution qui est non seulement utilisée par le gouvernement luxembourgeois, mais également par les banques les plus influentes de la place luxembourgeoise.

Cette solution fonctionne à partir de certificats d'authentification personnels délivrés par LuxTrust en tant qu'autorité de certification. C'est grâce à ces certificats que LuxTrust garantit l'identité de la personne qui, via un de ses produits, se connecte à une application en ligne pour effectuer des opérations électroniques.

En général, il se confirme que la coopération réciproque entre autorités et émetteurs est satisfaisante.

Pour ce qui est de la prévention, BEE SECURE (pour les jeunes et leur entourage) et CASES (pour les organismes et leurs employés) font un travail de sensibilisation et de formation intensives, et ce depuis plus de cinq ans.

L'échange des indicateurs de compromission ainsi que le travail proactif des CERT (GovCERT et CIRCL) sont importants pour la prévention au niveau des opérateurs. Les CERT proposent toujours à la victime de faire une remise volontaire de preuves. Ils sont par ailleurs capables de procéder à une collecte de telles preuves.

4.4.2 Ressources affectées à l'amélioration de la coopération

La Cellule de Renseignement Financier suit des formations régulières pour connaître les dernières évolutions technologiques. Elle est notamment membre du groupe de travail Egmont IEWG - Stream 3 "Financial Technologies and Transaction Innovation". Elle copréside, avec les États-Unis, un groupe de travail sur la fraude au président (dénommée selon la terminologie employée par les États-Unis "business e-mail compromise").

Pour ce qui est de la police, il faut constater que lorsqu'il est question d'une intrusion dans un système, il est généralement déjà trop tard pour empêcher le clonage des données. Une interception reste néanmoins envisageable, à condition que ces données réapparaissent de nouveau "en circulation", par exemple lorsqu'elles sont exposées en vente sur des sites de piratage. Si le traçage des adresses IP n'aboutit pas à une impasse, on tente de bloquer l'accès aux sites ou d'intercepter les acquéreurs opérant au moyen de ces références détournées.

Cette technologie de pointe liée au commerce des cartes de paiement (qui sera tôt ou tard remplacée par des applications pilotées par téléphone portable) est en évolution constante et exige de la part des forces de l'ordre qu'elles se familiarisent avec les innovations et les modes opératoires. Des conférences internationales pour experts permettent en outre d'échanger le savoir-faire et de privilégier les contacts entre les autorités chargées de lutter contre cette forme de délinquance.

Des réunions bilatérales ou des conférences portant sur la sécurité informatique sont organisées à cette fin. De plus, la fonction de "National Liaison Officer" auprès de l'ENISA étant assurée par un membre du GOVCERT, cela permet de créer des liens avec le secteur privé. Il est difficile de chiffrer le nombre de ressources investies, mais un effort constant est mené pour renforcer ou créer des liens avec le secteur privé.

4.5 Conclusions

La Police Judiciaire (SPJ) est toujours compétente pour les infractions de grande envergure ou chaque fois que des enquêtes techniques sont nécessaires. Le Service Régional d'Enquête Criminelle (SREC) est compétent au niveau territorial, mais si l'enquête est de grande envergure, c'est toujours le SPJ qui est compétent. La décision est prise par le parquet au cas par cas. Le SPJ dispose d'un département technique et scientifique, qui comprend deux sections (Nouvelles technologies et Police technique).

Selon les autorités nationales, les enquêtes portant sur des infractions en rapport avec des abus sexuels commis sur mineurs engendrent un volume de travail important pour la police technique (GSM, portables, ordinateurs qui sont utilisés pour commettre les infractions). C'est pourquoi la police considère qu'une cellule spéciale dédiée à la pédopornographie devrait être créée.

La section Nouvelles technologies de la Police grand-ducale est un exemple au niveau européen à la fois en ce qui concerne sa composition, ses missions et son positionnement au niveau international.

La possibilité que les spécialistes civils en informatique puissent acquérir la qualification d'officier de police judiciaire permet un rapprochement des compétences fort intéressant, qu'il serait opportun de développer au niveau européen.

Le service juridique informatique a été créé en 2003 afin d'offrir un appui spécialisé pour l'analyse des preuves numériques. En 2015, ce service a analysé un volume d'environ 300 térabits de données.

Le Parquet de Luxembourg compte des procureurs spécialisés en cybercriminalité. Au niveau des services d'instruction il y a un juge d'instruction qui s'occupe plus spécifiquement des affaires de cybercriminalité d'une certaine envergure et technicité au niveau du cabinet d'instruction.

Les obstacles à la lutte contre la cybercriminalité sont les mêmes que dans les autres pays européens. Il convient de noter qu'au niveau de certains praticiens l'absence de consensus sur la durée de conservation des données est considérée comme un élément bloquant.

Le partenariat public-privé est le véritable ciment de la lutte contre la cybercriminalité au Luxembourg. Les responsables hiérarchiques compensent les lacunes en termes de structure et de processus par les connaissances et les réseaux personnels.

Les différentes actions de sensibilisation ainsi que les outils d'analyse des risques et d'atténuation des cyberattaques sont clairement à mettre au crédit du Luxembourg.

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 Luxembourg a ratifié en 2014 la Convention de Budapest sur la cybercriminalité et son protocole par la loi du 18 juillet 2014 portant
1) approbation de la Convention du Conseil de l'Europe sur la cybercriminalité ouverte à la signature à Budapest le 23 novembre 2001,
2) approbation du Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, fait à Strasbourg le 28 janvier 2003,
3) modification du Code pénal,
4) modification du Code d'instruction criminelle,
5) modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

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

Le Luxembourg a établi, par la loi du 3 mars 2010, un régime général de responsabilité pénale des personnes morales, dont les articles pertinents du Code pénal sont les suivants:

Chapitre II-1. - Des peines applicables aux personnes morales

Art. 34. (L. 3 mars 2010) Lorsqu'un crime ou un délit est commis au nom et dans l'intérêt d'une personne morale par un de ses organes légaux ou par un ou plusieurs de ses dirigeants de droit ou de fait, la personne morale peut être déclarée pénalement responsable et encourir les peines prévues par les articles 35 à 38. La responsabilité pénale des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes infractions. Les alinéas précédents ne sont pas applicables à l'État et aux communes.

Art. 35. (L. 3 mars 2010) Les peines criminelles ou correctionnelles encourues par les personnes morales sont:

1) l'amende, dans les conditions et suivant les modalités prévues par l'article 36;

2) la confiscation spéciale;

3) l'exclusion de la participation à des marchés publics;

4) la dissolution, dans les conditions et suivant les modalités prévues par l'article 38.

Art. 36. (L. 3 mars 2010) L'amende en matière criminelle et correctionnelle applicable aux personnes morales est de 500 euros au moins. En matière criminelle, le taux maximum de l'amende applicable aux personnes morales est de 750 000 euros. En matière correctionnelle, le taux maximum de l'amende applicable aux personnes morales est égal au double de celui prévu à l'égard des personnes physiques par la loi qui réprime l'infraction. Lorsqu'aucune amende n'est prévue à l'égard des personnes physiques par la loi qui réprime l'infraction, le taux maximum de l'amende applicable aux personnes morales ne peut excéder le double de la somme obtenue par multiplication du maximum de la peine d'emprisonnement prévue, exprimée en jours, par le montant pris en considération en matière de contrainte par corps.

Art. 37. (L. 3 mars 2010) Le taux maximum de l'amende encourue selon les dispositions de l'article 36 est quintuplé lorsque la responsabilité pénale de la personne morale est engagée pour une des infractions suivantes:

- crimes et délits contre la sûreté de l'État
- actes de terrorisme et de financement de terrorisme
- infractions aux lois relatives aux armes prohibées en relation avec une association de malfaiteurs ou une organisation criminelle
- traite des êtres humains et proxénétisme
- trafic de stupéfiants en relation avec une association de malfaiteurs ou une organisation criminelle
- blanchiment et recel
- concussion, prise illégale d'intérêts, corruption active et passive, corruption privée
- aide à l'entrée et au séjour irréguliers en relation avec une association de malfaiteurs ou une organisation criminelle.
- (L. 21 décembre 2012) emploi illégal de ressortissants de pays tiers en séjour irrégulier en relation avec une association de malfaiteurs ou une organisation criminelle.

Art. 38. (L. 3 mars 2010) La dissolution peut être prononcée lorsque, intentionnellement, la personne morale a été créée ou, lorsqu'il s'agit d'un crime ou d'un délit puni en ce qui concerne les personnes physiques d'une peine privative de liberté supérieure ou égale à trois ans, détournée de son objet pour commettre les faits incriminés.

La dissolution n'est pas applicable aux personnes morales de droit public dont la responsabilité est susceptible d'être engagée. La décision prononçant la dissolution de la personne morale comporte le renvoi de celle-ci devant le tribunal compétent pour procéder à la liquidation.

Art. 39. (L. 3 mars 2010) Lorsque la personne morale encourt une peine correctionnelle autre que l'amende, cette peine correctionnelle peut être prononcée seule à titre de peine principale.

Art. 40. (L. 3 mars 2010) Lorsqu'un délit est puni de l'emprisonnement à l'égard des personnes physiques par la loi qui réprime l'infraction, la confiscation spéciale telle qu'elle est définie par l'article 31 peut être prononcée à titre de peine principale à l'égard de la personne morale, alors même qu'elle ne serait pas prévue par la loi particulière dont il est fait application.
La disposition de l'alinéa précédent ne s'applique pas en matière de délits de presse.

La législation luxembourgeoise ne prévoit pas de critères spécifiques qui permettraient de qualifier une infraction de type "cyber" de moins ou de plus grave et engendrer une réaction plus rapide et des devoirs plus poussés.

Néanmoins, plusieurs circonstances aggravantes sont prévues en la matière par les textes.
L'article 509-1 du CP (loi du 14 août 2000) prévoit une circonstance aggravante et, partant, des peines plus élevées lorsque l'accès ou le maintien frauduleux dans tout ou partie d'un système de traitement ou de transmission automatisé de données aura entraîné soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système.

En outre, l'article 509-4 du CP (loi du 10 novembre 2006) prévoit encore une augmentation des peines d'emprisonnement et d'amende "lorsque dans les cas visés aux articles 509-1 à 509-3, il y a eu transfert d'argent ou de valeur monétaire, causant ainsi une perte de propriété à un tiers dans un but de procurer un avantage économique à la personne qui commet l'infraction ou à une tierce personne".

Par ailleurs, en cas d'infractions commises par plusieurs personnes, le recours aux infractions d'association de malfaiteurs, sinon de bande organisée, demeure envisageable.

Les faits mineurs sont soit classés sans suites pénales, soit un avertissement avec un rappel à la loi est envoyé à l'auteur, soit le renvoi devant le Tribunal de simple police est sollicité auprès de la Chambre du conseil du tribunal d'arrondissement par application de circonstances atténuantes (jeune âge, faible préjudice, absence de casier judiciaire, première affaire...).

Quasiment tous les actes de cybercriminalité précèdent et constituent des actes préparatoires, soit d'une escroquerie ou d'une tentative d'escroquerie (par exemple CEO fraud), soit d'une extorsion ou d'une tentative d'extorsion (par exemple à l'aide de vidéos indélicates enregistrées sur des réseaux sociaux à l'insu des victimes).

Les infractions d'association de malfaiteurs, sinon de bande organisée, sont également susceptibles de venir se greffer à ces infractions si elles sont commises à plusieurs.

Il y a encore lieu de préciser que les infractions de cybercriminalité constituent des infractions primaires de blanchiment (article 506-1 du CP).

Par ailleurs, l'article 457 du CP couvre tous les commentaires et messages sur des réseaux sociaux de nature à inciter à la haine et à la violence contre un groupe déterminé non luxembourgeois.

Pour le moment, aucun changement de la législation actuelle sur la cybercriminalité n'est prévu.
Les textes revêtant une importance en matière de cybercriminalité sont :

- Le Code pénal
- Le Code d'instruction criminelle
- La loi du 15 juillet 1993 tendant à renforcer la lutte contre la criminalité économique et la fraude informatique

- La loi du 18 juillet 2014 portant approbation de la Convention du Conseil de l'Europe sur la criminalité ouverte à la signature à Budapest, qui a été transposée et a porté création des articles 509-1 à 509-6 du Code pénal
- La loi du 14 août 2000 relative au commerce électronique
- La loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel
- La loi modifiée du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques
- La loi du 11 août 1982 concernant la protection de la vie privée
- La loi du 18 avril 2001 sur les droits d'auteur, les droits voisins et les bases de données.

Dans le cadre des activités CIRCL, un "technical report" légal a été élaboré: il s'agit d'un bref résumé des articles de loi importants, comprenant un titre, les références de l'article, le domaine d'application, un exemple et les sanctions associées:

- https://circl.lu/pub/tr-44/

La directive 2013/40/UE[7] relative aux attaques contre les systèmes d'information a été transposée en droit interne par la loi du 18 juillet 2014 sur la cybercriminalité portant notamment approbation de la Convention du Conseil de l'Europe sur la cybercriminalité ouverte à la signature à Budapest le 23 novembre 2001.

Les textes pertinents figurent à l'annexe C du présent rapport.

[7] Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil (JO L 218 du 14.8.2013, p. 8).

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 loi du 21 février 2013 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants et portant modification de plusieurs dispositions du Code pénal transpose en droit national la directive 2011/93/UE, qui remplace la décision-cadre 2004/68/JAI et a pour objectif de rapprocher les législations des États membres de l'Union européenne en la matière afin de lutter le plus efficacement possible contre les abus sexuels, l'exploitation sexuelle des enfants et la pédopornographie, d'assurer la poursuite effective des infractions commises, de protéger les droits des victimes, de prévenir l'exploitation et les abus sexuels commis sur des enfants et, enfin, de mettre en place des systèmes de contrôle efficaces.

Dans la mesure où les dispositions de la directive précitée s'inspirent en effet étroitement de la Convention du Conseil de l'Europe sur la protection des enfants contre les exploitations et les abus sexuels ayant fait l'objet d'une approbation par la loi du 16 juillet 2011, qui a apporté une série de modifications au Code pénal luxembourgeois, la plupart des comportements prévus par la directive étaient déjà, depuis l'approbation de la Convention de Lanzarote, pénalement réprimés en droit luxembourgeois.

C/ Fraude en ligne aux cartes de paiement

Généralement, les sociétés émettrices de cartes de crédit (Six Payment, anciennement Cetrel) "imposent" à leurs clients d'aller déposer plainte à la police afin de pouvoir se faire rembourser les montants détournés, de sorte que le nombre de plaintes est considérable.

Par ailleurs, beaucoup de sociétés d'instruments financiers (Paypal), d'achat et de vente en ligne (Amazon), de même que les banques, procèdent à des déclarations de soupçon de blanchiment auprès de la Cellule de Renseignement Financier, qui adresse à son tour un rapport au parquet.

Le Luxembourg participe activement aux projets d'échange soutenus par la Commission européenne visant à communiquer – le plus rapidement possible – les données relatives au commerce électronique aux États membres concernés. Ce projet fonctionne depuis janvier 2015, sous le nom "FIU.NET Cross border reporting".

Si on ne prend en compte que les acteurs les plus importants exerçant leurs activités à partir du Luxembourg, plus de 7 500 échanges ont eu lieu entre le 1er janvier et le 30 avril 2016 (statistiques établies par Europol, gestionnaire de FIU.NET) avec les pays suivants: Allemagne 2 929, Royaume-Uni 2 863, Italie 462, France 368, Espagne 185, Pays-Bas 125, Belgique 99, Autriche 96, Pologne 90, Irlande 52, Lituanie 43, Roumanie 38, Portugal 35, Bulgarie 34, Suède 30, Danemark 29, Estonie 20, Croatie 16, Lettonie 16, Chypre 13, Hongrie 10, Finlande 9, Grèce 9, République tchèque 7, Slovaquie 6, Slovénie 5 et Malte 3.

La plupart de ces déclarations concernent des fraudes en ligne.

En principe, bon nombre de fraudes en ligne sont officiellement signalées aux autorités compétentes. Toutefois, les sociétés émettrices de cartes de paiement (ou les sociétés assurant la gestion des transactions effectuées au moyen de cartes de paiement) ne se manifestent généralement que sur la base des critères suivants:

i. s'il apparaît des indices particuliers, qui sont susceptibles de remonter à la source du "fléau" (identifier les protagonistes concernés) ou d'intervenir lorsque des complices tentent de faire usage de cartes encodées au moyen des références détournées;
ii. si le préjudice subi dépasse une certaine limite;
iii. si le mode opératoire mérite réflexion.

Cette restriction découle de l'ampleur considérable des fraudes commises au moyen de références de cartes de paiement, qui ont (comme chacun sait) atteint des sommets, dans le souci d'économiser des synergies et de canaliser / d'optimiser les efforts.

D/ Autres phénomènes de cybercriminalité

Pour ce qui est de la police, il faut constater que lorsqu'il est question d'une intrusion dans un système de cryptage, il est généralement déjà trop tard pour empêcher le clonage des données. Une interception reste néanmoins envisageable, à condition que ces données réapparaissent de nouveau "en circulation", par exemple lorsqu'elles sont exposées en vente sur des sites de piratage. Si le traçage des adresses IP n'aboutit pas à une impasse, on tente de bloquer l'accès aux sites, respectivement d'intercepter les acquéreurs opérant au moyen de ces références détournées.

Cette technologie de pointe liée au commerce des cartes de paiement (qui sera tôt ou tard remplacée par des applications pilotées par téléphone portable) est en évolution constante et exige de la part des forces de l'ordre qu'elles se familiarisent avec les innovations et les modes opératoires. Des conférences internationales pour experts permettent en outre d'échanger le savoir-faire et de privilégier les contacts entre les autorités chargées de lutter contre cette forme de délinquance.

5.2 Questions de procédure

5.2.1 Techniques d'investigation

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

Ces mesures sont prévues aux articles 31, 33 et 66 du CIC.

Comme expliqué ci-dessus, la suppression de données sur ordre du procureur ou du juge d'instruction sur la base des articles 33 et 66 du CIC est soumise aux conditions spécifiques suivantes:

- une copie des données a été préalablement établie,
- le support physique des données n'a pas été saisi,
- la détention ou l'usage des données est illégal ou dangereux pour la sécurité des personnes ou des biens,
- le support physique (par exemple l'ordinateur ou le serveur) abritant les données se situe au Grand-Duché de Luxembourg.

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

L'article 88-1 du CIC (loi du 26 novembre 1982) permet au juge d'instruction, à titre exceptionnel, par décision spécialement motivée et aux conditions qui y sont fixées, d'ordonner l'utilisation de moyens techniques de surveillance et de contrôle de toutes les formes de communication.

- la conservation de données informatiques

La conservation des données relatives au trafic:

Au Luxembourg, la collecte et la conservation des données relatives au trafic sont réglementées par la loi du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques.

Un règlement grand-ducal du 24 juillet 2010 déterminant les catégories de données à caractère personnel générées ou traitées dans le cadre de la fourniture de services de communications électroniques ou de réseaux de communications publics a précisé la notion de "données relatives au trafic".

La conservation rapide de données:

En la matière, l'article 48-25 du CIC permet la conservation rapide de données dans le cadre du flagrant délit ou de l'enquête préliminaire par le procureur d'État et dans le cadre de l'instruction par le juge d'instruction. La procédure pourra être utilisée aussi bien au niveau national qu'au niveau international dans le cadre de commissions rogatoires internationales.

En pratique, le procureur d'État ou le juge d'instruction demandera, directement ou par l'intermédiaire de la police, au détenteur des données (notamment un hébergeur) de conserver celles-ci pendant un délai de 90 jours. Les magistrats pourront formuler cette demande dans le cadre d'un dossier national ou à la suite d'une demande d'une autorité compétente étrangère.

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

Seul le juge d'instruction peut ordonner la saisie de données relatives au trafic (article 67-1 du CIC). Cette mesure doit être nécessaire à la manifestation de la vérité et les faits sur lesquels porte l'instruction doivent emporter une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement. Si une instruction judiciaire n'a pas (encore) été ouverte, le procureur d'État peut requérir du juge d'instruction qu'il ordonne ces mesures dans les conditions prévues à l'article 24-1 du CIC (mini-instruction).

La saisie de contenus obéit au droit commun des saisies. En pratique, cette saisie est toutefois ordonnée par un juge d'instruction, alors qu'elle s'accompagne généralement de la saisie de données relatives au trafic.

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

Le législateur national n'a pas fixé les modalités suivant lesquelles les fournisseurs de services doivent procéder à la divulgation rapide des données du trafic. Cette mesure nécessite par conséquent une ordonnance en bonne et due forme émise par un juge d'instruction.

Les notions relatives à la cybercriminalité ne sont pas spécialement définies par la législation luxembourgeoise. En pratique, les juridictions se réfèrent aux définitions données par les textes internationaux, dont la Convention de Budapest ainsi que son rapport explicatif.

Les données relatives au trafic sont définies par le règlement grand-ducal du 24 juillet 2010 déterminant les catégories de données à caractère personnel générées ou traitées dans le cadre de la fourniture de services de communications électroniques ou de réseaux de communications publics.
Pour ce qui est des notions de perquisition et de saisie, les définitions sont les mêmes que celles utilisées en droit commun.

Comme bonne pratique dans ce domaine, il convient de citer le fait qu'une enquête en matière de cybercriminalité se poursuit souvent en dehors des frontières du Luxembourg. Le résultat/succès des enquêtes en la matière dépend du retour rapide des demandes d'entraide internationale.

5.2.2 Examen criminalistique et chiffrement

En principe, les examens criminalistiques ne sont pas effectués par voie électronique ou à distance, sauf pour les exceptions suivantes:

- le suspect a donné son accord pour copier les données (par exemple compte d'un réseau social, comptes mails);
- si durant la perquisition, l'OPJ constate sur l'ordinateur du suspect une connexion ouverte dans le "cloud" et que le suspect ne donne pas son accord pour accéder à ses données, l'OPJ doit demander l'accord du juge d'instruction pour les copier.

Dans tous les autres cas, les données doivent être saisies via ordonnance ou d'une commission rogatoire internationale si les données se trouvent en dehors du territoire luxembourgeois.

Les examens technico-légaux (IT-Forensic) sont réalisés par la section Nouvelles technologies du SPJ. Pour l'examen des malwares trouvés, la section NT a recours, en fonction des situations, soit aux spécialistes du CIRCL, soit aux ressources mises à disposition par Europol-EC3 ou aux outils automatisés d'entreprises privées. En application du droit commun de la procédure criminelle, le recours à un expert judiciaire externe peut être ordonné en cas de besoin.

o Les techniques de chiffrement sont actuellement faciles à installer et utiliser. Terroristes, pédophiles et autres types de criminels s'en servent et sans mot de passe, il est quasi-impossible pour les experts de la PGD d'accéder aux contenus des disques durs. De plus, si le mot de passe est bien sélectionné, les attaques "brute-force" sont dès le début condamnées à l'échec.

o Les services de messagerie cryptent désormais toutes les conversations. Les messages et les appels sont désormais protégés avec le chiffrement d'un bout à bout et sont de ce fait indéchiffrables par les autorités de répression.

o Tous les smartphones de dernière génération ont des fonctions permettant de verrouiller l'accès et de crypter le contenu. Cette fonctionnalité est de plus en plus utilisée par les criminels. Si le suspect ne donne pas le code d'accès, le smartphone est inexploitable.

o Les sites les plus courants et les moteurs de recherche utilisent le protocole HTTPS pour chiffrer le trafic non décodable en cas d'interception.
Tous les domaines sont concernés, principalement le terrorisme, la pédopornographie et le trafic de stupéfiants. Le seul moyen d'accéder aux données, c'est de les capter avant le chiffrement. La mise en place d'un dispositif permettant de capter les données sur l'équipement du suspect n'est pas permise. Un projet de loi est en cours pour permettre aux autorités l'utilisation d'un tel dispositif dans le cadre d'affaires de terrorisme.

Au cas où un opérateur ou toute entreprise notifiée conformément à la loi du 27 février 2011 sur les réseaux et les services de communications électroniques utilise des procédés de codage, de compression ou de chiffrement, les informations interceptées sont à délivrer aux autorités légales en clair.

On ne dispose pas de centres spécialisés et le déchiffrement ne s'effectue pas en coopération avec des sociétés privées.

Le problème est toujours d'actualité pour tous les domaines précités et cruciaux, ainsi que dans les cas où la vie est en danger.

Un projet de loi visant à permettre aux autorités répressives d'utiliser un dispositif technique destiné à capter les données à distance avant le chiffrement est en cours d'examen.

5.2.3 E-evidence (preuves électroniques)

Si l'on considère la saisie pénale au sens classique du terme, c'est-à-dire placer un bien sous séquestre judiciaire, il est possible de saisir le matériel informatique hébergeant des données visées par une enquête ou une instruction judiciaire. Cette solution pragmatique se heurte toutefois essentiellement à deux problèmes:

- les données litigieuses peuvent être stockées sur un serveur qui abrite les données d'autres personnes que celle visée par l'enquête ou l'instruction. Tel est notamment le cas des hébergements mutualisés, où un serveur accueille les sites Internet d'une multitude de clients. La saisie touche non seulement la personne visée par l'enquête ou l'instruction, mais aussi l'hébergeur et toutes les autres personnes abritant légitimement leur site sur le serveur en question;
- la saisie du matériel informatique conduit à un blocage total de tous les contenus qui y sont stockés. La mesure n'étant pas ciblée, des contenus parfaitement licites mis en ligne par la personne visée par l'enquête ou l'instruction sont également bloqués.

La saisie physique du matériel informatique peut notamment être une solution en matière d'échanges de contenus à caractère pédopornographique par des connexions *peer-to-peer* initiées par des particuliers[8].

[8] Voir notamment TA Lux. 23.03.2011, n° 1059/2011; TA Lux. 07.10.2008, n° 2822/2008; TA Lux. 24.06.2008, n° 2126/2008; TA Lux. 06.11.2008, n° 3150/2008.

Par une loi du 18 juillet 2014[9], le législateur est intervenu pour encadrer plus spécifiquement la saisie de *"données stockées, traitées ou transmises dans un système de traitement ou de transmission automatisé de données"*[10]. Les articles 31, 33 (crimes et délits flagrants) et 66 (saisies ordonnées par un juge d'instruction) prévoient désormais expressément la saisie de données informatiques "*soit par la saisie du support physique de ces données, soit par une copie"*.

Si une copie est réalisée, les données utilisées comme preuve sont sauvegardées sur un support CD, DVD ou un disque dur en fonction du volume des données à saisir. À cet égard, il n'existe pas, en droit luxembourgeois, de contraintes spécifiques pour établir la preuve électronique.

La preuve en matière pénale est régie par le CIC. Il n'y a pas de conditions d'admissibilité particulières pour les preuves électroniques.

5.3 Protection des droits de l'homme / des libertés fondamentales

Les droits fondamentaux tels qu'ils découlent notamment de la CEDH et de la Charte des droits fondamentaux sont protégés par le fait que le système judiciaire luxembourgeois garantit un recours effectif à tout citoyen qui verrait un de ses droits fondamentaux violés.

9 Loi du 18 juillet 2014 portant 1) approbation de la Convention du Conseil de l'Europe sur la cybercriminalité ouverte à la signature à Budapest le 23 novembre 2001, 2) approbation du Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, fait à Strasbourg le 28 janvier 2003, 3) modification du Code pénal, 4) modification du Code d'instruction criminelle, 5) modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

10 Depuis la loi du 15 juillet 1993 tendant à renforcer la lutte contre la criminalité économique et la fraude informatique, ayant introduit les infractions en matière informatique dans le Code pénal, le législateur se réfère aux termes "système de traitement ou de transmission automatisé de données" pour désigner les "systèmes informatiques" (terminologie employée par la Convention de Budapest) dans les différents textes répressifs.

Plus spécifiquement en matière de protection des données, la commission nationale de protection des données (CNPD) doit:

o contrôler et vérifier la légalité de la collecte et de l'utilisation des données soumises à un traitement et informer les responsables du traitement quant à leurs obligations;

o veiller au respect des libertés et droits fondamentaux des personnes, notamment au respect de la vie privée, et informer le public sur les droits des personnes concernées;

o recevoir et examiner les plaintes et demandes de vérification de la licéité des traitements;

o assurer l'application des dispositions de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et de ses règlements d'exécution.

Les articles 33 et 66 du CIC permettent au procureur, en cas de flagrance, et au juge d'instruction, en cas d'information judiciaire, de faire supprimer des données stockées, traitées ou transmises dans un système de traitement ou de transmission automatisé de données, à condition que:

- une copie des données ait été préalablement établie,
- le support physique des données n'ait pas été saisi,
- la détention ou l'usage des données soit illégal ou dangereux pour la sécurité des personnes ou des biens,
- le support physique (par exemple l'ordinateur ou le serveur) abritant les données se situe au Grand-Duché de Luxembourg.

Parallèlement aux impératifs en matière de preuve, la condition selon laquelle une copie des données effacées doit avoir été préalablement établie permet de rétablir celles-ci en cas d'annulation de la décision d'effacement par la chambre du conseil ou par les juridictions du fond, ainsi qu'en cas de non-lieu ou d'acquittement prononcé sur le fond de l'affaire. Ainsi que l'explique le législateur, "la décision d'effacement ne peut pas être assimilée à une sanction de confiscation anticipée. Il s'agit soit d'une protection des personnes et des biens contre de nouvelles infractions (en cas de malware notamment), soit d'une mesure tendant à éviter la propagation de matériel illégal (tel que la pédopornographie). En cas d'acquittement ou de décision de ne pas procéder à des poursuites, les données saisies (leur copie) pourront être restituées. En cas de poursuites, en revanche, les données seront confisquées".

À la lecture des travaux parlementaires, on constate que l'idée du législateur était de rendre des données illicites ou dangereuses inaccessibles, en attendant une décision au fond. Les contenus pouvant être bloqués sont notamment "la pédopornographie, les malwares ou encore l'incitation à la haine, voire le terrorisme".

Des recours sont prévus contre toutes ces mesures.

5.4 Compétence

5.4.1 Principes appliqués pour enquêter sur la cybercriminalité

L'article 7-2 du CIC répute avoir été "commise sur le territoire du Grand-Duché de Luxembourg toute infraction dont un acte caractérisant un de ses éléments constitutifs a été accompli au Grand-Duché de Luxembourg".

La jurisprudence a précisé les termes de cet article en retenant que "l'élément à prendre en considération comme critère de localisation est l'élément matériel. Cet élément est pris en considération tant au regard de la conduite délictueuse que du résultat produit par l'acte". Pour donner compétence aux juridictions luxembourgeoises "il suffit donc qu'un des actes caractérisant l'un des éléments des infractions ait été accompli sur le territoire national (…). Il convient dès lors de déterminer le lieu de commission de l'infraction, c'est-à-dire de localiser les différents éléments composant les infractions dans l'espace, tout en retenant qu'il suffira pour attribuer la compétence aux juridictions luxembourgeoises que soit l'action, soit le résultat ait été réalisé sur le territoire luxembourgeois". Il faut signaler encore un arrêt de la Cour d'appel du 11 mars 2008, qui a exigé que l'acte caractérisant un des éléments constitutifs doit avoir été commis "en entier" sur le territoire luxembourgeois pour donner compétence aux juridictions nationales.

Il ressort de la jurisprudence liée à l'application de ce texte qu'il suffit que le dommage résultant de l'infraction ait été subi au Luxembourg pour que la compétence des juridictions nationales soit établie.

En matière d'escroquerie, il a notamment été jugé que "les tribunaux indigènes sont compétents pour juger un prévenu de nationalité luxembourgeoise ou étrangère qui a commis au Grand-Duché des manœuvres frauduleuses au moyen desquelles une escroquerie a été commise à l'étranger ou qui a encaissé au Luxembourg des fonds provenant d'une escroquerie commise à l'étranger". Les juridictions luxembourgeoises sont encore compétentes si "les actes préparatoires de l'escroquerie ou bien l'entrée en possession des fonds par l'escroc [ont] eu lieu au Grand-Duché de Luxembourg (…), indépendamment du fait que le contrat ait été signé à l'étranger et que le dessaisissement de l'argent se soit fait à l'étranger". En revanche, les actes qualifiés de préparatoires de l'escroquerie, comme la mise au point d'un montage ou les actes postérieurs à la remise, ne constituent pas des actes caractérisant un des éléments constitutifs de l'infraction au sens de l'article 7-2 du CIC.

Les mêmes règles s'appliquent en matière d'abus de confiance, d'extorsion, de faux et d'usage de faux et de participation à une association de malfaiteurs.

La criminalité informatique constituant désormais expressément une infraction primaire du délit de blanchiment, l'article 506-3, premier alinéa, du CP retient la compétence territoriale des juridictions luxembourgeoises même si l'infraction primaire a été commise à l'étranger.

La Convention de Budapest prévoit également que la compétence territoriale doit être établie si une des infractions qu'elle définit est commise par un ressortissant luxembourgeois, à condition que l'infraction soit punissable également là où elle a été commise ou qu'elle ne relève de la compétence territoriale d'aucun État. Cette extension de la compétence des juridictions nationales pour les infractions commises par un ressortissant luxembourgeois à l'étranger est réglée par l'article 5 du CIC.

Le législateur a encore complété l'article 7-4 du CIC en prévoyant que les infractions en matière informatique commises à l'étranger pourront être poursuivies au Luxembourg lorsque le suspect n'est pas extradé par le pays requis. Le Luxembourg élève ainsi la criminalité informatique au rang des affaires soumises au principe "aut dedere aut judicare" (extrader ou poursuivre).

Parallèlement aux textes légaux encadrant la compétence territoriale des autorités luxembourgeoises chargées des poursuites, il y a lieu de mentionner les chefs de compétence d'origine jurisprudentielle.
En premier lieu, il existe des cas de prorogation de compétence "lorsqu'il existe entre des infractions ressortissant à des juridictions différentes un lien si étroit qu'il est dans l'intérêt d'une bonne justice que toutes ces infractions soient jugées par le même juge (Encyclopédie Dalloz, Pénal, v° compétence, n° 254).

Ces cas de prorogation de la compétence internationale des juridictions nationales sont ceux de la connexité et de l'indivisibilité, où en raison d'un lien logique, plus ou moins étroit, entre plusieurs infractions, le juge compétent pour juger les unes est aussi compétent pour juger les autres, alors même qu'à l'égard de celles-ci, envisagées seules et en elles-mêmes, il ne le serait peut-être pas (Roger Thiry, Précis d'instruction criminelle en droit luxembourgeois, T. I, n° 375)".

Il y a notamment prorogation de compétence dans le cas d'une infraction commise à l'étranger et dans un même laps de temps, déterminée par le même mobile et qui procède de la même cause que les infractions commises sur le territoire luxembourgeois. Tel est le cas s'il existe un rapport logique entre le fait commis à l'étranger et ceux commis au Grand-Duché de Luxembourg, dans la mesure où les infractions commises au Grand-Duché de Luxembourg ne doivent leur existence qu'à l'infraction commise à l'étranger.

Un autre chef de compétence est constitué par les infractions collectives, qui se caractérisent "par plusieurs faits, constituant chacun une infraction, mais qui peuvent former une activité criminelle unique, parce que liées entre elles par une unité de conception et de but". En cas d'infraction collective, "il suffit, pour rendre compétents les tribunaux répressifs luxembourgeois, que l'un des actes caractérisant un des éléments constitutifs de l'infraction se soit produit dans le Grand-Duché de Luxembourg, et il n'est pas relevant que les actes composant ces éléments constitutifs aient été perpétrés par un seul agent ou par plusieurs".

5.4.2 Règles en cas de conflit de compétence et lorsqu'il est fait appel à Eurojust

Il va de soi que, dans le cadre d'une bonne administration de la justice, il est opportun qu'un seul État centralise les dossiers à l'encontre d'un même auteur si cela est compatible avec la législation interne (compétence territoriale, prorogation de compétence et incrimination).

Dans le cas contraire, cela pourrait conduire à des jugements contradictoires et, le cas échéant, à l'application du principe non bis in idem s'il devait s'avérer que les mêmes faits ont été poursuivis dans plusieurs États en même temps.

En pratique, les États se mettent d'accord et procèdent à une dénonciation des faits en bonne et due forme par l'intermédiaire des autorités centrales (parquet général au Luxembourg). La coopération avec Eurojust est également très fréquente et le Luxembourg est membre du Cybercrime Network d'Eurojust.

Afin d'apprécier l'opportunité de dénoncer un dossier, plusieurs critères sont pris en compte par le parquet: nationalité et localisation de l'auteur, nationalité de la victime, hauteur du préjudice, état d'avancement de l'enquête, respect des droits de la défense, etc.

Le Luxembourg n'a pas mis en œuvre de 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.

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

L'article 33, cinquième alinéa, et l'article 66, troisième alinéa, du CIC prévoient que "la saisie des données stockées, traitées ou transmises dans un système de traitement ou de transmission automatisé de données peut se faire, soit par la saisie du support physique de ces données, soit par une copie de ces données". Le texte ne faisant pas de distinction selon que les données se trouvent au Luxembourg ou à l'étranger, il est admis que toutes les données accessibles à partir du Luxembourg peuvent y être saisies sous forme de copie.

En revanche, l'effacement de ces données est soumis à la condition que les données concernées soient stockées au Luxembourg.

En ce qui concerne la police, aucun problème spécifique ne s'est posé dans le cadre d'enquêtes en rapport avec la cybercriminalité.

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

Selon la police, les instruments d'entraide judiciaire internationale sont trop lents et insuffisants pour combattre efficacement la cybercriminalité. Face à la volatilité des preuves sur Internet et la diversité de la durée de rétention des données d'un État à l'autre, une réaction rapide et des instruments souples sont requis.

5.5 Conclusions

Le Luxembourg a ratifié en 2014 la Convention du Conseil de l'Europe sur la cybercriminalité et son protocole additionnel.

Le Luxembourg a aussi transposé la Directive 2013/40/UE relative aux attaques contre les systèmes d'information et la Directive 2011/93/UE 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.

En ce qui concerne l'usurpation d'identité, les dispositions pertinentes s'appliquent également pour les vols d'identité sur les réseaux sociaux (il existe déjà une jurisprudence dans ce domaine - deux condamnations, une pénale et une autre administrative).

La compétence dans ces cas est établie dès qu'il existe un élément constitutif de l'infraction commis au Luxembourg. Ni la double incrimination, ni la condition de la plainte de la victime, ni une dénonciation officielle ne sont requises.

Le juge d'instruction peut autoriser des techniques d'investigation comme les écoutes téléphoniques, l'infiltration, l'expertise informatique, le repérage des télécommunications ou la saisie de données informatiques. La conservation rapide des données peut être autorisée par la police, le procureur ou le juge d'instruction. La saisie du contenu dans le "cloud" est possible si les données sont accessibles à partir du Luxembourg.

Les praticiens considèrent que la législation en matière de pédopornographie constitue un outil satisfaisant.

De nombreuses évolutions de la législation sont en cours (captation de données à distance, enquête sous pseudonyme, reforme du Service de Renseignement). Il convient souligner que la reforme du Service de renseignement a été entre temps finalisée après la visite d'évaluation. En outre il n'y a pour le moment pas de modifications prévues de la législation en matière de cybercriminalité.

6 ASPECTS OPÉRATIONNELS

6.1 Cyberattaques

6.1.1 Nature des cyberattaques

Les statistiques de la police concernant la cybercriminalité reprennent tous les faits enregistrés de manière informatique sous la catégorie "cybercrime". Cette catégorie regroupe diverses infractions: manipulation illégale d'un système informatique, fraude bancaire par Internet, escroquerie par Internet, etc. Vu la diversité de ces faits, il est impossible de donner des chiffres exacts sur les différentes formes de cybercriminalité, comme par exemple les "cyberattaques".
Au total 715 affaires ont été enregistrées sous la catégorie "cybercrime" en 2014 et 1 190 affaires en 2015.

6.1.2 Mécanisme de réaction aux cyberattaques

Le Haut-Commissariat à la Protection Nationale coordonne la réponse aux cyberattaques. Il dispose aussi d'une cellule d'évaluation de la menace, dénommée CERC (Cellule d'évaluation des risques cyber). Il existe aussi des organes de gestion de crise: le Single Point of Contact Cyber (SPOC Cyber), la Cellule d'évaluation du risque cyber (CERC) et la Cellule de crise Cyber.

La police a recours aux instruments d'entraide judiciaire internationale, aux échanges directs d'informations dans les limites de la législation nationale et internationale, aux échanges via Europol et Interpol, aux échanges de contacts personnels (entre services de police) et à la communication volontaire d'informations par les fournisseurs de services de communication.

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

Le Luxembourg ne possède pas de banque de données identifiant les victimes.
À ce jour, on n'a pas encore répertorié de cas de victimes au Luxembourg dont les images à caractère pédopornographique ont été diffusées sur Internet.

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

Le Luxembourg s'est doté d'un article de loi spécifique visant à lutter contre le phénomène du "grooming" (pédopiégeage).

L'article 385-2 du CP (loi du 16 juillet 2011) dispose en effet que le simple fait pour un majeur de faire des propositions sexuelles à un mineur de moins de seize ans ou à une personne se présentant comme telle en utilisant un moyen de communication électronique est puni d'un emprisonnement d'un mois à trois ans et d'une amende de 251 à 50 000 euros.

Lorsque les propositions ont été suivies d'une rencontre, des peines plus élevées sont prévues par l'article précité, à savoir un emprisonnement d'un à cinq ans et une amende de 251 à 75 000 euros.
Le sujet fait partie intégrante des sessions de sensibilisation BEE SECURE. Une campagne spécifique sur le cyber harcèlement a déjà eu lieu en 2011 et une nouvelle campagne est en préparation pour l'année scolaire 2016/17, avec comme sujet principal le combat du "hate speech" sur Internet.

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

Dans ce cadre, il y a lieu de mentionner l'association ECPAT Luxembourg, qui a pour mission de lutter par tous les moyens légaux contre l'exploitation sexuelle des enfants à des fins commerciales ainsi que de sensibiliser et informer l'opinion publique sur les droits de l'enfant en la matière. Cette association facilite l'identification et la mise en œuvre de programmes en faveur des enfants vulnérables et/ou victimes d'exploitation sexuelle à des fins commerciales et de leur famille.

Par ailleurs, il y a également lieu de citer BEE SECURE, une initiative commune du Ministère de l'Economie, du Ministère de la Famille, de l'Intégration et à la Grande Région et du Ministère de l'Education nationale, de l'Enfance et de la Jeunesse. BEE SECURE est opérée par trois partenaires: Service national de la jeunesse, KannerJugendTelefon et securitymadein.lu.

L'initiative BEE SECURE englobe les actions au niveau de la sensibilisation à une utilisation plus sécurisée des nouvelles technologies de l'information et de communication.

BEE SECURE est aussi un projet cofinancé par la Commission Européenne et fait fonction de centre de sensibilisation luxembourgeois au sein du réseau paneuropéen Insafe. La hotline nationale BEE SECURE Stopline, opérée par le KannerJugendTelefon, est membre du réseau international INHOPE - International Association of Internet Hotlines.

Par ailleurs, le site childprotection.lu a été mis en place et a pour objectif de sensibiliser le public aux différentes formes d'abus et d'exploitation sexuels des mineurs et de leur permettre de signaler des cas soupçonnés.

Le KannerJugendTelefon (opérateur de BEE SECURE Stopline) et la Police Grand-Ducale ont coopéré avec ECPAT Luxembourg (initiateur du projet) dans le cadre d'une campagne de sensibilisation contre le tourisme sexuel impliquant des enfants (childprotection.lu et dépliants et affiches papier).

À l'occasion de la campagne précitée, le cadre légal et les moyens de dénonciation ont été communiqués au grand public, et une collaboration avec les opérateurs de tourisme du Luxembourg a été engagée.

Au Luxembourg, aucun cas de "spectacle pornographique" n'a à ce jour été décelé par les autorités judiciaires.

BEE SECURE Stopline se chargerait d'émettre des alertes qui permettraient aux autorités d'agir le plus rapidement possible.

La Cellule de Renseignement Financier travaille en étroite coopération avec les établissements de paiement et de monnaie électronique afin de détecter les transactions relatives à cette forme de criminalité. Au cours de l'année 2015, une demi-douzaine de déclarations d'opérations suspectes a été reçue sur ce sujet. Celles-ci ont été analysées en coopération avec les cellules de renseignement des pays concernés.

Une coopération plus étroite avec Europol est actuellement mise en place à ce niveau.

- la mise en place de lignes d'urgence et la fourniture d'informations spécifiques sur la marche à suivre pour déposer une plainte.

Toute personne voulant informer respectivement déposer une plainte concernant des abus sexuels contre des enfants sur Internet peut accéder, via l'interface www.police.lu, à un commissariat virtuel et y déposer sa plainte, qui sera traitée par des enquêteurs spécialisés dans les meilleurs délais. le site de la BEE SECURE Stopline (stopline.bee-secure.lu) permet a chaque citoyen à travers un formulaire interactif de dénoncer de manière anonyme des contenus d'abus sexuels sur mineurs. Ces dénonciations sont alors traitées selon les procédures opérationnelles de la BEE SECURE Stopline et transmises a la Police Grand-Ducale.

- la mise au point d'outils d'information à destination des enfants pour une utilisation sûre de l'internet.

L'initiative BEE Secure, opérée par le Service national de la jeunesse, KannerJugendTelefon et securitymadein.lu organise régulièrement des séances d'information pour jeunes ayant comme but la sensibilisation aux éventuels risques possibles lors de la navigation sur Internet.

- la mise au point d'outils d'information sur les comportements préjudiciables/illicites sur Internet.

L'initiative BEE Secure dispose a travers la BEE SECURE Stopline d'une plateforme stopline.bee-secure.lu pour dénoncer de manière anonyme des contenus illicites sur Internet tels que contenus d'abus sexuels sur mineurs, contenus racistes, révisionnistes et discriminatoires et contenus terroristes. Pour d'autres contenus illicites les utilisateurs peuvent contacter de manière anonyme et confidentielle le service BEE SECURE Helpline au numéro gratuit 80021234.

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

L'article 33, cinquième alinéa, et l'article 66, troisième alinéa, du CIC autorisent la suppression et donc le blocage de données dont la détention ou l'usage est illégal ou dangereux pour la sécurité des personnes ou des biens.

Les contenus pouvant être bloqués sont notamment "la pédopornographie, les malwares ou encore l'incitation à la haine, voire le terrorisme".

La mesure est entourée d'importantes garanties, en ce qu'elle doit être ordonnée par le procureur d'État en cas de flagrant crime ou délit et par un juge d'instruction dans tous les autres cas. Ces décisions peuvent faire l'objet de recours en annulation et en restitution.

Le KannerJugendTelefon comme operateur de la BEE Secure Stopline est membre de INHOPE (International Association of Internet Hotlines). La mission de cette association est de soutenir et d'améliorer la collaboration entre les différentes "hotlines" en vue d'un traitement rapide et efficace des signalements de contenus d'abus sexuels sur mineurs.

Il y a transfert de notifications sur les contenus d'abus sexuels sur mineurs par la BEE SECURE Stopline aux autorités nationales si les contenus sont hébergés au Luxembourg et au réseau international INHOPE si les contenus sont hébergés dans un pays avec une hotline partenaire du réseau INHOPE. Les notifications sur des contenus racistes, révisionnistes et discriminatoires et contenus terroristes sont transmis aux autorités nationales.

La limitation de responsabilité dont bénéficient les hébergeurs, prévue à l'article 62 de la loi sur le commerce électronique, s'accompagne de l'obligation pour ces prestataires, dès qu'ils ont connaissance de contenus illicites stockés sur leur infrastructure, d'agir promptement pour retirer ces contenus ou rendre leur accès impossible.

D'une façon générale, les hébergeurs luxembourgeois bloquent les contenus qui sont manifestement illicites dans les pays de l'Union Européenne. On peut entre autres citer le matériel pédopornographique et les propos qui incitent manifestement à la haine (notamment raciale) ou à la commission d'actes terroristes.

Afin d'accroître leur sécurité juridique, de nombreux hébergeurs définissent les contenus illicites dans leurs conditions générales. Cet encadrement juridique, au moyen de conventions de droit privé, leur permet notamment de bloquer des œuvres artistiques mises en ligne en violation des droits d'auteur d'autrui ou des programmes malveillants diffusés par leurs systèmes informatiques.

Dans le cadre de la gestion des signalements de contenus illégaux, BEE SECURE Stopline, ainsi que les entités en charge du service, sont considérées comme des "relais de signalement" entre le public et les autorités compétentes. Ainsi, dès que BEE SECURE Stopline transmet un contenu illicite au service de police compétent, celui-ci se charge de faire bloquer/enlever ce contenu.

Le secteur privé est coopératif en cas de notification d'un contenu illégal, et en principe le contenu concerné est retiré rapidement.

Les hébergeurs peuvent prendre connaissance de contenus illicites en effectuant des contrôles spontanés ou en s'appuyant sur les dénonciations émanant de toute personne intéressée. Il faut rappeler, à cet égard, le service BEE SECURE Stopline grâce auquel tout particulier peut dénoncer des contenus relatifs à la pornographie infantile, au racisme, au révisionnisme et à d'autres discriminations, ainsi qu'au terrorisme. Dans le cadre de la gestion des signalements de contenus illégaux, BEE SECURE Stopline dispose d'un accord de collaboration avec la police judiciaire qui lui permet d'agir en tant que relais et expert pour la réception, l'analyse et la transmission de renseignements aux services adéquats de la police. La décision finale sur la légalité ou l'illégalité d'un contenu signalé à BEE SECURE Stopline et la décision d'en informer l'hébergeur en cas d'hébergement au Luxembourg appartient aux autorités chargées des poursuites, en l'occurrence la Police Grand-Ducale ou le parquet. En général, BEE SECURE Stopline ne contacte pas directement l'hébergeur en cas de retrait de contenus illicites, sauf si la Police Grand-Ducale en fait la demande.

Initiés dans le cadre de la coopération entre les autorités de police et le secteur privé, les blocages sont généralement exécutés sur la base des conditions générales de l'hébergeur, qui se réserve expressément le droit de retirer de ses systèmes des contenus illicites.

Le cas échéant, le procureur peut ordonner le blocage d'un contenu sur le fondement de l'article 33, cinquième alinéa, et de l'article 66, troisième alinéa, du CIC.

L'article 62 de la loi sur le commerce électronique oblige l'hébergeur à retirer les informations ou à rendre l'accès à celles-ci impossible. Sur la base de cet article, le prestataire pourrait dès lors décider d'effacer définitivement les données litigieuses. En pratique, celui-ci efface les données sur l'infrastructure accessible via Internet, mais en garde une copie de sauvegarde. Il procède donc à un blocage des données.

Il existe un accord de collaboration entre la Police Grand-Ducale de Luxembourg, le Service National de la Jeunesse Luxembourg (SNJ) et le KannerJugendTelefon (KJT) concernant le service de la BEE SECURE Stopline, qui s'inscrit dans le cadre de l'initiative BEE SECURE. Chaque fois que ce service découvre un site illicite ou est informé par ses homologues internationaux de l'existence d'un tel site, celui-ci en informe les services de police compétents en la matière. Ceux-ci s'engagent à enlever respectivement à bloquer le site concerné dans un délai assez court (de préférence en 48 heures si possible de point de vue d'investigation).

Dans le cas de contenus à caractère pédopornographique hébergés dans d'autres pays, les procédures opérationnelles de BEE SECURE Stopline prévoient d'en informer la Police Grand--Ducale et de transmettre les liens pertinents à une hotline partenaire, membre du réseau INHOPE (International Association of Internet Hotlines). Il est à noter dans ce contexte que INHOPE bannit le terme "pédopornographie" et lui préfère l'expression "matériel d'abus sexuel contre mineurs" (ou "contenus ayant trait à la violence sexuelle exercée contre des enfants"), l'équivalent de "Child sexual abuse material" en anglais.

Le but du travail de BEE SECURE Stopline et des membres du réseau INHOPE est le retrait le plus rapidement possible des contenus d'abus sexuels sur mineur afin d'éviter la revictimisation des enfants et adolescents représentés sur les images et vidéos ("Notice and Takedown").

Dans les cas où le serveur est situé en dehors du Luxembourg et dans un Etat avec une hotline partenaire INHOPE (International Association of Internet hotlines), l'agence BEE SECURE Stopline transmet les données à ses homologues internationaux concernés ainsi qu'à la Police Grand-Ducale. Dans le cas ou le server est situé en dehors du Luxembourg et dans un Etat sans hotline partenaire INHOPE, la BEE SECURE Stopline transmet les données à la Police Grand-Ducale et dans la base de données de INHOPE ICCAM. En cas d'urgence ou d'événement de grande envergure ou à caractère spécial, les autorités policières informent leurs homologues européens du contenu illicite découvert par le biais des systèmes Interpol/Europol.

Ily a transfert des notifications sur les images d'abus sexuels sur mineurs par la BEE SECURE Stopline aux autorités nationales (contenu hébergé au Luxembourg) si les contenus sont hébergés au Luxembourg et au réseau international INHOPE (contenu hébergé à l'étranger) si les contenus sont hébergés dans un pays avec une hotline partenaire du réseau INHOPE. Les notifications sur des contenus racistes, révisionnistes et discriminatoires et contenus terroristes sont transmis aux autorités nationales.

Le parquet de Luxembourg dispose de trois magistrats qui, en plus des affaires de jeunesse, s'occupent plus particulièrement des affaires de pédopornographie.
Au niveau de la police, le SPJ protection de la jeunesse s'occupe également plus spécifiquement de ces affaires.

ECPAT et BEE SECURE s'occupent de la détection, de l'information du grand public et de la dénonciation des faits aux autorités judiciaires.

6.3 Fraude en ligne aux cartes de paiement

Généralement, les sociétés émettrices de cartes de crédit (Six Payment, anciennement Cetrel) "imposent" à leurs clients d'aller déposer plainte à la police afin de pouvoir se faire rembourser les montants détournés, de sorte que le nombre de plaintes est considérable.

Par ailleurs, beaucoup de sociétés d'instruments financiers (Paypal), d'achat et de vente en ligne (Amazon), de même que les banques, procèdent à des déclarations de soupçon de blanchiment auprès de la Cellule de Renseignement Financier, qui adresse à son tour un rapport au parquet.

Le Luxembourg participe activement aux projets d'échange soutenus par la Commission Européenne visant à communiquer – le plus rapidement possible – les données relatives au commerce électronique aux États membres concernés. Ce projet fonctionne depuis janvier 2015, sous le nom "FIU.NET Cross border reporting".

Si on ne prend en compte que les acteurs les plus importants exerçant leurs activités à partir du Luxembourg, plus de 7 500 échanges ont eu lieu entre le 1er janvier et le 30 avril 2016 avec d'autres pays (statistiques établies par Europol, gestionnaire de FIU.NET).

Les banques, de même que les établissements de paiement et de monnaie électronique, doivent respecter les dispositions édictées par la loi du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme portant transposition de la directive 2001/97/CE du Parlement européen et du Conseil du 4 décembre 2001 modifiant la directive 91/308/CEE du Conseil relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux (ci-après la "loi LB/FT").

La Cellule de Renseignement procède à de nombreux échanges internationaux en cette matière, afin de faire parvenir les informations concluantes à l'État membre concerné le plus rapidement possible.

- accroître la sécurité des paiements autres qu'en espèces et réduire la vulnérabilité des bandes magnétiques

Les établissements de paiement et de monnaie électronique doivent appliquer les mesures de vigilance imposées par la loi LB/FT. L'analyse des transactions effectuée par la cellule de renseignement financier a révélé que dans de très nombreux cas, les transactions frauduleuses sont bloquées avant que le gain escompté par le criminel ne lui ait été reversé.

- renforcer les procédures d'autorisation des transactions en ligne et l'authentification des clients

Mise en place du système "3D secure", aussi connu sous les appellations commerciales "Verified By Visa" et "MasterCard SecureCode".

La sécurisation des données électroniques et des transactions effectuées en ligne a également été renforcée par l'entrée en vigueur de la loi sur le commerce électronique, le 14 août 2000, et le règlement grand-ducal portant sur la signature électronique, qui définit les caractéristiques que celle-ci doit revêtir pour être reconnue comme légale (1er juin 2001).

Avec la création de LuxTrust S.A., dont deux tiers du capital sont détenus par l'État, une solution de sécurisation électronique commune a été mise en place, solution qui est non seulement utilisée par le gouvernement luxembourgeois, mais également par les banques les plus influentes de la place luxembourgeoise.

Cette solution fonctionne à partir de certificats d'authentification personnels délivrés par LuxTrust en tant qu'autorité de certification. C'est grâce à ces certificats que LuxTrust garantit l'identité de la personne qui, via un de ses produits, se connecte à une application en ligne pour effectuer des opérations électroniques.

En général, il se confirme que la coopération réciproque entre autorités et émetteurs est satisfaisante.

6.4 Conclusions

Si la réaction à l'exploitation sexuelle de mineurs s'effectue facilement via l'association BEE SECURE et son partenariat avec les hébergeurs, les discussions avec ceux-ci sont moins productives pour ce qui est des autres thématiques (comme les cyberattaques et les fraudes à la carte bancaire).

Toutes les infractions de pédopornographie relèvent de la compétence du parquet de la jeunesse. Celui-ci compte cinq juges d'instruction spécialisés dans ce type d'infractions. Les dénonciations ou les plaintes émanent de tiers, de parents ou d'enseignants. Dans 90 % des cas, les délinquants sont condamnés. La législation actuelle ne permet pas à un enquêteur de se substituer à la victime, mais un projet de loi permettra à l'avenir les enquêtes sous pseudonyme.

Les enquêteurs participant à la protection des mineurs ne font pas l'objet d'un suivi psychologique, mais ils en auraient besoin.

L'exemple luxembourgeois en ce qui concerne la lutte contre l'exploitation sexuelle des enfants est fort intéressant, qu'il s'agisse de la réponse pénale apportée ou du fait qu'il est également tenu compte de l'enfant sous une forme représentée (images et représentations virtuelles).

Cependant, l'absence de veille des services de police chargés de ce domaine due au cadre légal ne permet pas une détection proactive. D'autre part l'absence d'outil de recoupement et de bases de données destinées à éviter la revictimisation est de nature à affaiblir les efforts opérationnels déployés en la matière.

La lutte contre la fraude en ligne souffre des mêmes problèmes structurels liés à l'absence de spécialisation des enquêteurs.

Il n'existe pas au sein de la police de veille pour détecter les infractions en ligne (technique "mapping peer to peer" ou cyberpatrouilles).

Selon les autorités de police, les infractions à la carte bancaire les plus fréquentes sont les fraudes, les escroqueries, les chèques falsifiés et les faux ordres de virement. L'entraide judiciaire est considérée comme trop lente et insuffisante, tandis que la plateforme de communication Europol est jugée très utile.

7 COOPÉRATION INTERNATIONALE

7.1 Coopération avec les agences de l'UE

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

Aucune formalité particulière ne doit être respectée pour ce qui est de la coopération entre les autorités nationales luxembourgeoises et Europol/EC3, Eurojust et l'ENISA en matière de cybercriminalité. Les dites autorités doivent toutefois toujours respecter le droit national luxembourgeois.

D'une façon générale, la coopération s'effectue par le biais d'un juge d'instruction.

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

- SECURITYMADEIN.LU participe, en collaboration avec Europol, à un projet de lutte contre les attaques de type "phishing": EU-PI - https://phishing-initiative.eu/
- Au niveau de l'ENISA, et dans le cadre du programme de soutien aux CERT, des échanges réguliers ont lieu avec CIRCL, GOVCERT et les autres CERT du Luxembourg.

Le Luxembourg est membre du Cybercrime Network d'Eurojust.

La police coopère de manière constante avec Europol/EC3 en échangeant le plus grand nombre d'informations possible. Citons, à titre d'exemple, deux cas, dont le premier est plus ancien et le deuxième, plus récent, fait toujours l'objet d'investigations.

1. Botnet Citadel

En 2013, des informations transmises par Europol ont permis de saisir des serveurs C2 utilisés pour le botnet Citadel. De plus, grâce aux précisions techniques fournies par Europol, l'exploitation du matériel saisi a été facilitée.

2. Actuellement, le Grand-Duché, à l'instar de beaucoup d'autres pays, est touché par le cheval de Troie bancaire Dridex. Un échange constant d'éléments découverts grâce aux analyses réalisées a permis d'établir plusieurs liens avec des cas dans d'autres pays.

Les différentes réunions organisées au niveau d'Eurojust permettent un échange de bonnes pratiques en matière de cybercriminalité. La connaissance personnelle des acteurs de terrain permet de connaître les bons procédés et d'adresser directement toute demande à la personne compétente.

La cybercriminalité étant un phénomène international, la lutte contre ce genre de criminalité ne peut être gagnée qu'au moyen d'un échange continu et souple d'informations. Le Grand-Duché, qui possède un secteur bancaire assez important et un secteur ICT en croissance, ne peut que profiter des possibilités de coopération mises à disposition par des institutions comme Europol.

Le Luxembourg ne participe pas au groupe stratégique de l'Union européenne regroupant, sous l'égide d'Europol, les chefs des services nationaux de lutte contre la criminalité utilisant les technologies avancées ni à d'autres formes de coopération concrète (y compris aux cyberpatrouilles).

7.1.3 Résultats opérationnels des ECE et des cyberpatrouilles

Les forces de l'ordre procèdent à des échanges de renseignements. En 2014 et 2015, le Grand-Duché a activement participé, avec la France et la Belgique, à un groupe d'enquête mixte placé sous la tutelle d'une "Équipe commune d'enquête". Cette opération a abouti à l'arrestation des membres d'un réseau criminel opérant à grande échelle dans le domaine du détournement de carburant.

7.2 Coopération entre les autorités luxembourgeoises et Interpol

Actuellement le Luxembourg, en l'occurrence la section de protection de la jeunesse du service de police judiciaire est compétente en la matière et n'a pas recours à la base de données d' Interpol ICSE (International child sexual exploitation data base) dans le cadre des investigations nationales. Ayant accès à l'ICSE, la section en question est en principe tenue non seulement de consulter régulièrement la base de données mais devrait aussi transmettre le matériel illicite (p.ex. photos pédopornographiques et valeurs HASH) saisi lors d'une procédure judiciaire, ceci en vue d'identifier les victimes et les auteurs potentiels par le biais de la coopération internationale.

7.3 Coopération avec des pays tiers

En ce qui concerne la politique à l'égard des pays tiers en matière de prévention de la cybercriminalité et d'enquêtes, le Ministère public transmet les dossiers dans lesquels un compte tiers a pu être mis en évidence, sans que l'auteur soit connu ou identifiable, à la Cellule de renseignement financier, qui en informe son homologue du pays concerné afin que des mesures soient prises pour bloquer ou fermer le compte en question.

Par ailleurs, les dossiers de fraude en ligne à la carte de crédit sont transmis de manière généralisée au SPJ, section Criminalité générale, aux fins de la centralisation et du traitement des informations recueillies au sein d'Eurojust/d'Europol en vue d'une enquête d'envergure à ce sujet.

Il est aussi prévu de transmettre à Interpol les dossiers de type escroquerie dite "nigériane" ("sexting" ou "sextape"), dans lesquels une adresse IP dans un pays tiers a pu être identifiée, afin de signaler le délit au pays tiers concerné et de mettre en évidence d'éventuels recoupements au niveau international.

Europol/EC3/Eurojust représentent une précieuse valeur ajoutée en ce qui concerne la coordination entre les différentes institutions des pays tiers lors d'affaires de grande envergure et pour ce qui est de l'échange d'informations.

7.4 Coopération avec le secteur privé

Les succursales locales des sociétés privées coopèrent sur une base volontaire en ce qui concerne les informations BSI (basic subscriber information). Ils ne communiquent cependant pas les informations a leur disposition s'ils jugent que les données n'ont pas de lien avec le Luxembourg. Le cas échéant, pour saisir ces données BSI et les contenus, ou en cas de non-coopération, la PGD se voit obligée de demander au juge d'instruction l'émission de commissions rogatoires internationales, qui ralentissent considérablement les résultats.

Le Luxembourg participe notamment au système FIU.NET Cross border. Il est également représenté auprès d'Eurojust et d'Europol.

7.5 Instruments de la coopération internationale

7.5.1 Entraide judiciaire

a. Dans la mesure où l'entraide judiciaire en matière de cybercriminalité implique le plus souvent la communication de données détenues par des tiers (par exemple données bancaires, données relatives à l'identification du titulaire d'un compte Internet ou d'une adresse IP) et nécessitent la réalisation d'actes coercitifs, c'est la loi modifiée du 8 août 2000 sur l'entraide judiciaire internationale en matière pénale qui s'applique. Cette loi est applicable à toute demande d'entraide judiciaire en matière pénale qui tend à faire opérer au Grand-Duché une saisie d'objets, de documents, de fonds, de biens de toute nature, une perquisition ou tout autre acte d'instruction présentant un degré de contrainte analogue.

La loi du 8 août 2000 s'applique à l'égard :

– des autorités judiciaires d'États requérants qui ne sont pas liés au Grand-Duché de Luxembourg par un accord international en matière d'entraide judiciaire;

– des autorités judiciaires d'États requérants qui sont liés au Grand-Duché de Luxembourg par un accord international en matière d'entraide judiciaire, à moins que les dispositions de la présente loi soient contraires à celles de l'accord international; et

– d'une autorité judiciaire internationale reconnue par le Grand-Duché de Luxembourg.

b. Lorsque la demande d'entraide judiciaire n'implique pas, pour son exécution, d'actes coercitifs (par exemple audition d'une personne, communication de procès-verbaux de police, communication de données figurant dans les bases de données des autorités policières ou judiciaires, communication des données publiques), l'exécution se fait sur la base des seules conventions internationales et, en l'absence de celles-ci, sur la base de la réciprocité.

Pour les demandes d'entraide judiciaire en matière pénale émanant de l'étranger, la procédure à suivre varie selon que la demande d'entraide comporte ou non l'exécution de mesures coercitives.

a. Dans le premier cas, la loi du 8 août 2000 sur l'entraide judiciaire internationale en matière pénale est applicable, et la demande d'entraide doit être adressée au parquet général près la Cour supérieure de justice, qui est l'autorité centrale au Luxembourg chargée de recevoir les demandes d'entraide dont l'exécution implique des actes coercitifs.

Le parquet général transmet la demande d'entraide, accompagnée de son avis basé sur la loi du 8 août 2000, au parquet du tribunal d'arrondissement territorialement compétent en fonction du lieu où l'exécution de la demande d'entraide doit avoir lieu (Tribunal d'arrondissement de Luxembourg ou de Diekirch). Le parquet saisit ensuite le juge d'instruction aux fins d'exécution de la demande d'entraide.

Aux fins de la transmission à l'autorité requérante des pièces saisies en exécution de la demande d'entraide, le Ministère public doit saisir la chambre du conseil du tribunal d'arrondissement de réquisitions à cet effet. La chambre du conseil statue sur la régularité de la procédure et la transmission des pièces et documents saisis à l'autorité requérante. Aucun recours ne peut être exercé contre cette décision.

b. Dans le deuxième cas, la demande d'entraide est exécutée directement par le parquet du tribunal d'arrondissement territorialement compétent, qui transmet le dossier à la police pour exécution des devoirs sollicités, sans passer par l'autorité centrale.

En ce qui concerne les demandes d'entraide judiciaire en matière pénale nationales envoyées à l'étranger, ces demandes sont établies soit par les parquets, en cas d'enquête préliminaire, soit par le juge d'instruction, en cas d'information judiciaire.

Ces demandes sont le plus souvent envoyées directement à l'autorité judiciaire de l'État requis (lorsque des conventions internationales prévoient cette voie de communication), sinon elles sont transmises à l'autorité judiciaire requérante par la voie officielle, par le biais du parquet général, avec, le cas échéant, l'intervention du ministère de la justice et du ministère des affaires étrangères.

Les demandes d'entraide judiciaire sont reçues et envoyées par courrier postal, courrier électronique ou par télécopie.

Il convient par ailleurs de noter que le Luxembourg dispose d'un bureau de recouvrement des avoirs ("ARO"), qui est chargé de recevoir, par la voie du programme SIENA (mis en place par Europol), les demandes d'informations préalables à l'envoi d'une demande d'entraide judiciaire.

Les conditions sont différentes si la demande d'entraide comporte ou non l'exécution de mesures coercitives.

Si l'exécution de la demande d'entraide ne comporte pas de devoirs coercitifs, celle-ci est exécutée sans autres conditions.

Si l'exécution de la demande d'entraide comporte des devoirs coercitifs, la loi du 8 août 2000 sur l'entraide judiciaire internationale en matière pénale est applicable, et la demande d'entraide doit, sous réserve de dispositions plus favorables prévues par les conventions internationales, réunir les conditions suivantes (article 5 de la loi du 8 août 2000):

- elle doit émaner d'une autorité judiciaire compétente en vertu du droit de l'État requérant;
- le fait à la base de la demande doit être susceptible d'être qualifié de crime ou de délit, punissable d'une peine privative de liberté d'un maximum d'au moins une année en vertu de la loi luxembourgeoise et de la loi de l'État requérant;

- la personne visée par la demande ne doit pas avoir été jugée au Grand-Duché de Luxembourg pour le même fait;
- la mesure sollicitée doit pouvoir être prise en vertu du droit luxembourgeois par les autorités judiciaires luxembourgeoises à des fins de recherches ou de poursuites comme s'il s'agissait d'une affaire interne analogue;
- la prescription de l'action publique ne doit pas avoir été acquise, ni d'après la loi luxembourgeoise, ni d'après la loi de l'État requérant.

D'un point de vue formel, la demande d'entraide doit contenir les indications suivantes (article 4 de la loi du 8 août 2000):

- l'autorité dont émane la demande;
- l'objet et le motif de la demande;
- la date et le lieu de la commission des faits, un exposé sommaire des faits et le lien entre ces faits et l'objet de l'acte d'instruction sollicité;
- dans la mesure du possible, l'identité et la nationalité de la personne en cause;
- le nom et l'adresse du destinataire, s'il y a lieu;
- le texte de l'inculpation et des sanctions y attachées;
- une traduction en langue française ou allemande de la demande d'entraide et des pièces à produire.

La demande d'entraide peut, en outre, être refusée sur décision du Parquet Général dans les cas suivants (article 3 de la loi du 8 août 2000):

- si la demande d'entraide est de nature à porter atteinte à la souveraineté, à la sécurité, à l'ordre public ou à d'autres intérêts essentiels du Grand-Duché de Luxembourg;
- si la demande d'entraide a trait à des infractions susceptibles d'être qualifiées par la loi luxembourgeoise soit d'infractions politiques, soit d'infractions connexes à des infractions politiques;
- si la demande d'entraide a trait à des infractions en matière de taxes et d'impôts, de douane ou de change en vertu de la loi luxembourgeoise.

La demande d'entraide peut également être refusée (article 4 de la loi du 8 août 2000, condition de proportionnalité) si, sans devoir procéder à un examen du fond, il est prévisible que les moyens à mettre en œuvre ne sont pas aptes à réaliser l'objectif visé à la demande d'entraide ou vont au-delà de ce qui est nécessaire pour l'atteindre.

Il est à noter que plusieurs conventions internationales auxquelles le Luxembourg est partie prévoient des conditions d'application plus souples:

Ainsi, en vertu de la convention d'application de l'accord de Schengen,

- le fait à la base de la demande doit être punissable d'une peine privative de liberté d'un maximum d'au moins six mois seulement en vertu de la loi luxembourgeoise au lieu d'un an prévu par la loi,
- la condition de proportionnalité prévue à l'article 4 de la loi du 8 août 2000 et celle de prescription prévue à l'article 5 ne sont pas applicables.

La transmission à l'autorité requérante des documents et objets saisis exige l'accord de la chambre du conseil du tribunal d'arrondissement, qui statue en même temps sur la régularité de la procédure par une ordonnance non susceptible de recours. Elle statue dans un délai de vingt jours de sa saisine.

La loi du 8 août 2000 prévoit en son article 8 que les demandes d'entraide judiciaire sont traitées comme affaires urgentes et prioritaires.

L'article 2 de la loi du 8 août 2000 prévoit que si l'affaire paraît grave et s'il y a urgence consistant en particulier en un risque de dépérissement de preuve, l'autorité judiciaire peut procéder aux devoirs d'instruction sollicités sans transmettre la demande au préalable au procureur général d'État.

Les demandes d'entraide comportant des mesures coercitives sont exécutées en général dans des délais de l'ordre de quelques mois.

Pour les demandes très urgentes (risque immédiat d'atteinte à la vie ou à l'intégrité physique), il est arrivé que la procédure ait été exécutée et que les pièces d'exécution aient été communiquées à l'autorité requérante (par voie électronique) dans les 24 heures'.

Les types d'action les plus fréquents sont les demandes d'identification de titulaires de comptes électroniques ou d'adresses IP.

Les faits à la base de l'entraide en matière de cybercriminalité sont le plus souvent les suivants:

- usage abusif de cartes de paiement ou de comptes électroniques en rapport avec des paiements sur Internet,
- escroquerie commise via Internet,
- consultation en ligne de matériel pédopornographique,
- extorsion (menace de révéler des enregistrements vidéo compromettants réalisés par webcam).

Afin de s'assurer que leur demande d'entraide remplisse les conditions exigées par la législation luxembourgeoise, certains pays (par exemple le Japon) envoient systématiquement, de manière informelle et par voie électronique, des projets de demande d'entraide à l'autorité centrale afin de recueillir son avis.

Des consultations informelles avec les autorités compétentes d'un autre État membre ont parfois lieu lors d'enquêtes d'e grande envergure. Dans ce cas, les canaux utilisés sont soit des relations personnelles, soit des canaux mis à disposition par Europol/Interpol.

Au niveau informel, les réseaux européens (TF-CSIRT - https://www.terena.org/activities/tf-csirt/) et internationaux des CERT (FIRST - https://www.first.org/) constituent un outil efficace et utile en termes d'entraide, de détection et de prévention de cyberattaques.

L'entraide en matière de cybercriminalité est accordée notamment sur la base des traités suivants:

Conventions multilatérales:

- Convention de Budapest sur la cybercriminalité du 23 novembre 2001,
- Convention européenne d'entraide judiciaire en matière pénale du 20 avril 1959,
- Convention d'application de l'accord de Schengen du 14 juin 1985,
- Convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne.

Conventions bilatérales:

- Traité d'entraide judiciaire en matière pénale entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement des États-Unis d'Amérique du 13 mars 1997,
- Traité d'entraide judiciaire en matière pénale entre le Grand-Duché de Luxembourg et l'Australie du 24 octobre 1988.

En l'absence de traités, l'entraide est accordée sur la base de la réciprocité et sous réserve du respect des conditions prévues par la loi du 8 août 2000.

La police a recours aux instruments d'entraide judiciaire internationale, aux échanges directs d'informations dans les limites de la législation nationale et internationale, aux échanges via Europol et Interpol, aux échanges de contacts personnels (entre services de police) et à la communication volontaire d'informations par les fournisseurs de services de communication.

7.5.2 Instruments de la reconnaissance mutuelle

Le Luxembourg n'a pas eu recours aux instruments de la reconnaissance mutuelle de l'UE dans le cadre de la prévention, des enquêtes et des poursuites pour des faits de cybercriminalité.

7.5.3 Remise/Extradition

Le mandat d'arrêt européen est régi en droit luxembourgeois par la loi du 17 mars 2004 relative au mandat d'arrêt européen et aux procédures de remise entre États membres de l'Union européenne.
Il y a lieu de préciser qu'il n'existe pas de régime spécifique pour les faits de cybercriminalité, qui sont d'ailleurs dans leur globalité susceptibles de constituer le fondement d'un mandat d'arrêt européen à condition d'être punissable d'une peine d'emprisonnement d'un maximum d'au moins douze mois lorsque le mandat est émis aux fins de poursuites et lorsqu'une condamnation à une peine est intervenue ou qu'une mesure de sûreté a été infligée, pour des sanctions prononcées d'une durée d'au moins quatre mois.

Par ailleurs, il y a lieu de noter que la cybercriminalité fait également partie des infractions permettant l'exécution d'un mandat d'arrêt européen sans contrôle de la double incrimination.

La loi du 17 mars 2004 prévoit en ses articles 4 et 5 les cas dans lesquels l'exécution du mandat peut être refusée.

L'exécution du mandat d'arrêt européen relève de la compétence du Ministère Public qui le transmet à la police aux fins de notification et d'exécution.

Après notification, la personne doit être présentée dans les 24 heures au juge d'instruction, qui, à l'issue d'un bref interrogatoire, décerne un mandat de "maintien en détention".

La procédure diffère alors selon que la personne concernée est d'accord ou non avec sa remise.
En cas d'accord, la personne doit être remise à l'autorité requérante dans les dix jours.

À défaut d'accord, la chambre du conseil du tribunal d'arrondissement doit être saisie par voie de réquisition du Ministère Public et statue sur la remise dans les vingt jours.

Les échanges se font entre les autorités requérantes et requises émettrices des mandats (juge d'instruction, parquet et police en tant que service exécutant) par voie directe (téléphone, courriel, courrier).

Aucune procédure spécifique n'est prévue en ce qui concerne les demandes liées à la cybercriminalité.
L'article 6 de la loi du 17 mars 2004 prévoit 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.

La personne recherchée peut dès lors être arrêtée provisoirement sur la base du signalement visé à l'alinéa précédent sans que le mandat d'arrêt soit encore émis.

Néanmoins, la personne devra être présentée dans les 24 heures au juge d'instruction, à défaut de quoi elle devra être remise en liberté.

En théorie, la personne pourrait également faire l'objet d'une rétention policière d'une durée de quatre heures.

Le temps de réponse dépend du fait de savoir si la personne a ou non été présentée aux autorités et si le dossier est complet.

7.6 Conclusions

En ce qui concerne la coopération avec les pays tiers, les autorités nationales ont fait état d'essais, tous infructueux, avec certains pays africains.

Pour ce qui est de la coopération avec le secteur privé, d'autres problèmes ont été signalés s'agissant de la coopération avec certains ISP importants. Les États-Unis d'Amérique s'opposent souvent à communiquer des données concernant les infractions relatives aux appels à la haine, se retranchant derrière la liberté d'expression.

Compte tenu du fait que la majorité des demandes provenant de l'étranger nécessitent une autorisation judiciaire afin d'obtenir des éléments de réponse, les commissions rogatoires internationales sont considérées comme étant plus rapides et plus efficaces que les demandes d'assistance mutuelle.

Les autorités de police ont également fait une suggestion concernant l'utilité de créer, au niveau de l'Union Européenne, un point de contact pour les relations avec des multinationales importantes. Bien que ce service existe au sein d'Europol, il conviendrait de mieux le promouvoir.

Malgré la taille de l'État, et proportionnellement aux ressources disponibles, la participation des services de police à la collaboration internationale avec Europol dans le cadre des groupes EMPACT, EUCTF et ECTEG pourrait être plus intense.

8 FORMATION, SENSIBILISATION ET PRÉVENTION

8.1 Formation spécifique

L'ERA propose des formations intéressantes en la matière. La section Nouvelles technologies du SPJ dispense des formations à l'intention des magistrats, notamment des présentations portant sur les nouveaux outils utilisés par les auteurs d'infractions de type cyber (Darknet, bitcoin, etc.).

Par ailleurs, Microsoft a également déjà organisé des formations s'adressant aux magistrats du parquet.

La Cellule de Renseignement participe activement aux groupes de travail Egmont afin d'appréhender les risques liés à l'utilisation des nouvelles technologies dans le milieu financier (bitcoin, paiement en ligne, paiement mobile, etc.).

À l'École de police, la cybercriminalité est abordée lors de la formation de base et des formations continues des policiers et des enquêteurs.

Il n'existe pas de modules de formation spécialisés ciblant les experts judiciaires en TI et les enquêteurs s'occupant des affaires de cybercriminalité.

Étant donné qu'il s'agit de formations spécialisées, la section Nouvelles technologies organise et coordonne elle-même les formations techniques. Ce sont surtout les formations gratuites ou à coûts réduits proposées par Europol, Interpol ou les agences de police voisines qui sont suivies par les membres de la section NT. Les formations spécialisées proposées par le secteur privé ayant généralement un coût élevé, dans la mesure du possible, un seul membre de la section NT y participe et agit ensuite en tant que "démultiplicateur". Des sessions de formation interne sont ainsi organisées quatre ou cinq fois par an afin de partager les connaissances acquises.

Au niveau des magistrats, une formation continue est offerte dans le cadre des contrats conclus entre l'École nationale de la magistrature (France) et le Luxembourg. Des formations sont également offertes dans le cadre de l'ERA (Europäische Rechtsakademie) à Trèves. Le parquet général agit en tant qu'autorité coordinatrice dans le domaine de la formation des magistrats. Le Luxembourg participe également au REFJ (Réseau européen de formation judiciaire).

Les coûts annuels de formation de la police grand-ducale en matière de cybercriminalité se chiffrent à 15 000 euros approximativement.

L'Université de Luxembourg ne prévoit pas de cours spécifiques sur la cybercriminalité. Elle organise toutefois des colloques sur cette question.

De plus, l'Université de Luxembourg propose un master professionnel en gestion de la sécurité des systèmes d'information et le Lycée des Arts et Métiers propose des programmes consacrés à la cybersécurité dans le cadre de son BTS informatique.

8.2 Sensibilisation

L'initiative BEE SECURE sensibilise chaque année plus de 10 000 élèves et étudiants fréquentant les écoles fondamentales et secondaires, ainsi que les parents, les enseignants et les éducateurs, au moyen de séances d'information et de formations ciblées. Les campagnes annuelles menées par BEE SECURE permettent en outre de sensibiliser le grand public sur un sujet spécifique.

Un programme de sensibilisation consacré aux séniors a été lancé en 2014 sous la dénomination Silver Surfer, en collaboration avec le Ministère de la Famille.

L'initiative BEE SECURE vise les plus jeunes, ainsi que le personnel encadrant/ les enseignants, les éducateurs qui travaillent avec des personnes de cette classe d'âge et, évidemment, les parents. Lancées en 2013, les histoires illustrées de Bibi et ses amis s'adressent aux enfants âgés de 5 à 8 ans. Ce projet a d'ailleurs été primé lors de l'ECPA Award 2015 organisé par le Réseau européen pour la prévention de la criminalité.

8.3 Prévention

8.3.1 Législation/politique nationale et autres mesures

La prévention ne fait pas partie des missions du GOVCERT. L'État a confié cette mission, menée avec le soutien de CASES, à l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Depuis 2003, avec la création de CASES dans le cadre du plan directeur de la sécurité des systèmes d'information et de communication, une politique de prévention, de sensibilisation et de formation en sécurité de l'information est menée.

L'initiative BEE SECURE est née de cette volonté et sensibilise, tous les ans, plus de 10 000 élèves des écoles fondamentales et secondaires, ainsi que des parents, enseignants et éducateurs, par des séances d'informations et formations ciblées. En plus les campagnes annuelles de BEE SECURE permettent de sensibiliser le grand public sur un sujet spécifique.

Un programme de sensibilisation consacré aux séniors a été lancé en 2014 sous la dénomination Silver Surfer, en collaboration avec le Ministère de la Famille.

CASES se concentre sur la formation initiale et continue des agents de l'État et propose ses services au secteur privé, en partenariat avec des instituts de formation (par exemple House of Training).

CIRCL soutient et forme les équipes opérationnelles aux techniques de "réponse sur incident" et de détection d'intrusions.

8.3.2 Partenariat public/privé (PPP)

CERT.LU est un exemple phare du partenariat public-privé des CERT au Luxembourg. Onze entités en font partie, quatre du secteur public et sept du secteur privé.

Les campagnes BEE SECURE, qui sont proposées à un rythme annuel, bénéficient d'un large soutien du secteur privé en ce qui concerne la diffusion des messages.

8.4 Conclusions

Le Luxembourg peut faire valoir un très grand nombre d'expériences qu'il serait utile de diffuser plus largement auprès des États membres et des institutions.

BEE SECURE, qui fait partie d'INHOPE, est un projet commun à différents ministères, piloté par un comite interministériel. BEE SECURE organise des sessions de sensibilisation qui s'adressent aux enfants, aux parents et aux adultes, à la demande des communes ou des écoles. Ces campagnes s'articulent chaque année autour d'un thème différent. En 2015-2016, le sujet retenu était intitulé "Clever cloud user". Un atelier destiné aux enfants vise également à apprendre comment se comporter de manière sécurisée sur Internet.

BEE SECURE Helpline offre des services Internet et participe activement à l'ICCAM, dans le cadre d'un échange d'informations entre différentes helplines sur les contenus d'abus sexuels sur mineurs. BEE SECURE Helpline a aussi conclu un accord opérationnel avec la police luxembourgeoise pour filtrer les sites Internet.

Une ligne téléphonique - KJT - est mise à la disposition des enfants et des jeunes pour obtenir une assistance. KJT possède aussi un site de signalement anonyme des contenus illégaux sur Internet (abus sexuels sur mineurs, racisme, discrimination, terrorisme).

SecurityMadein.lu est un autre site consacré aux activités de sensibilisation et de prévention. Ses trois pôles d'activité sont Aware, CASES et CIRCL.

À titre d'exemple, à la date de la visite, six sessions à l'intention des personnes âgées avaient déjà été organisées (pour un total de 100 participants) dans le cadre du projet Silver Surfer, ainsi que onze événements s'adressant aux enfants (plus de 500 participants).

DFIR, un CERT qui s'adresse aux entreprises, organise mensuellement des petits-déjeuners réunissant une cinquantaine de participants.

CASES, outre le projet MONARC, organise des activités de prévention et d'accompagnement des entreprises, y compris des formations dans les administrations publiques. Des actions ponctuelles sont organisées au profit des administrations communales (analyse de risque, mise en place de la charte de sécurité et formation).

Dans le domaine de la prévention, CIRCL, qui a été créé en 2007 et s'adresse aux communes et au secteur privé, développe une approche pragmatique, ouverte et innovante. Outre les projets précités, BGP ranking, MISP et autres, cette structure a conduit 1 400 investigations techniques à la suite d'incidents qui lui avaient été signalés.

9 REMARQUES FINALES ET RECOMMANDATIONS

9.1 Suggestions du Luxembourg

Le Luxembourg est conscient de l'importance d'Internet pour l'économie et a mis en place de nombreux acteurs dans le domaine de la prévention, détection et réaction. La coopération ainsi que la coordination fonctionnent grâce aux outils, services et méthodes mis à la disposition des acteurs, mais aussi grâce aux événements organisés pour fédérer la coopération dans ce domaine.

Comme exemples de bonnes pratiques peuvent être cités les suivants:

- MONARC, une méthode d'analyse des risques qui promeut la collaboration et réduit ainsi de 80 % l'effort individuel au niveau des analyses de risques;
- BGP ranking, méthode de collecte des "black listes" et d'évaluation du facteur malicieux AS, HCPN, plan d'intervention d'urgence;
- MISP, une plateforme d'échange d'indicateurs de compromission;
- les sensibilisations à large échelle effectuées par CASES et BEE SECURE (BEE SECURE possède un degré de notoriété au sein de la population de plus de 60 %);
- les sessions de sensibilisation obligatoires et facultatives dans les établissements scolaires;
- les CERT.

On trouvera ci-après quelques suggestions émanant du Luxembourg pour renforcer la lutte contre la cybercriminalité:

- créer un point de contact européen, des règles et des procédures identiques pour l'échange des données avec les grands fournisseurs de services de communications en dehors de l'UE;
- faciliter et accélérer l'exécution des commissions rogatoires internationales;
- créer une taxonomie commune et identique concernant la classification et les statistiques dans le domaine de la cybercriminalité;
- renforcer la coopération avec le secteur privé et le monde académique;
- créer un modèle de référence en définissant des standards minimums en matière de structure et de fonctionnement des unités d'enquête cybercrime, cyberpatrouille et cyberprévention.

9.2 Recommandations

Le Luxembourg devrait procéder à un suivi des recommandations figurant dans le présent rapport 18 mois après l'évaluation 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 luxembourgeoises. Elle a en outre présenté, sur la base des différentes bonnes pratiques, des recommandations à l'UE, à ses institutions et agences, et notamment à Europol.

9.2.1 Recommandations adressées au Luxembourg

Le Luxembourg devrait:

1. créer et alimenter des statistiques plus consolidées qui permettraient une meilleure connaissance du phénomène de la cybercriminalité;
2. développer davantage la partie opérationnelle de la Stratégie nationale de cybersécurité;
3. réfléchir à se doter d'outils techniques et légaux pour effectuer des opérations d'infiltration et des enquêtes sous pseudonyme dans le cyberespace;
4. considérer à créer la base légale pour permettre le blocage des sites au contenu illégal;
5. renforcer les effectifs de la police judiciaire pour permettre les approches transversales et les spécialisations;
6. contribuer à alimenter les bases internationales de données des victimes de pédopornographie;

7. continuer et renforcer la coopération judiciaire et policière internationale, surtout en ce qui concerne l'échange d'informations;
8. continuer à mettre en place des formations à l'intention des enquêteurs et des procureurs concernant les phénomènes criminels liés aux techniques IT, y compris en contribuant aux synergies apportées par ECTEG, CEPOL et Interpol;
9. offrir un soutien psychologique structurel aux policiers traitant les dossiers de pédopornographie.

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

Les États membres devraient s'inspirer des bonnes pratiques identifiées par l'équipe d'évaluation au Luxembourg, à savoir:

- la très bonne collaboration entre le secteur public et le secteur privé;
- l'existence de procureurs spécialisés en cybercriminalité;
- le recrutement et le plan de carrière des spécialistes des nouvelles technologies;
- le dynamisme en matière de recherche et développement et le partage des résultats avec les différents acteurs;
- la politique répressive en matière de pédopornographie;
- l'approche holistique en matière de sensibilisation;
- le rôle des institutions dans la recherche des fuites de données (surtout CIRCL).

9.2.3 Recommandations adressées à Eurojust/Europol/ENISA

Europol devrait:

- mieux promouvoir les services mis à la disposition des États Membres;

ANNEXE A: PROGRAMME DE LA VISITE SUR PLACE

Programme de la visite sur place effectuée au Luxembourg du 7 au 9 juin 2016

Lundi 6 juin 2016

Arrivée des experts au Luxembourg

Mardi 7 juin 2016

8h30 Départ des experts de l'hôtel (transport assuré par la Police Grand-Ducale)

9h00-12h00 Salle de réunion du Parquet Général du Luxembourg (Cité judiciaire)

- 9h00-9h10 Accueil des experts par Madame le Procureur général d'État
- 9h10-10h30 Introduction générale de l'évaluation avec explication du dispositif luxembourgeois en matière de cybercriminalité et de cybersécurité (tour de table) (en présence de représentants de tous les acteurs participant à l'évaluation)
- 10h30-10h45 Pause café
- 10h45-11h15 Présentation du dispositif luxembourgeois en matière de cybersécurité (M. F. Thill)
- 11h15-12h00 Textes légaux et mise en œuvre de la Convention de Budapest

12h00-14h00 Pause déjeuner

14h00-18h00 Salle de réunion du Parquet Général du Luxembourg (Cité judiciaire)

- 14h00-14h30 Dispositif du parquet en matière de cybercriminalité
- 14h30-15h30 Entraide judiciaire en matière de cybercriminalité
- 15h30-15h45 Pause café
- 15h45-16h30 Présentation sur les discours de haine sur Internet
- 16h30-17h00 Présentation sur la pédopornographie sur Internet
- 17h00-18h00 Cellule de renseignement financier (CRF) et cybercriminalité; formation des magistrats

18h00 Retour des experts à l'hôtel

Mercredi 8 juin 2016

8h30 Départ des experts de l'hôtel

9h00-13h00 Salle de réunion de la police judiciaire, rue de Bitbourg, à Hamm

- 9h00-9h15 Organigramme
- 9h15-9h45 Coopération internationale
- 9h45-10h00 Pause café
- 10h00-10h20 Fraudes à la carte bancaire
- 10h20-10h40 Escroquerie sur Internet
- 10h40-10h55 Pause café
- 10h55-12h00 Formation
- 12h15-12h45 Enquêtes en matière de cybercriminalité: exemple
- 12h45-13h00 Résumé et séance de questions-réponses

13h00-14h30 Pause déjeuner

14h30-18h00 Salle de réunion du SNJ, 138 bd. de la Pétrusse

- 14h30-14h50 Présentation des activités de sensibilisation du grand public (BEE SECURE)
- 14h50-15h20 Présentation de la BEE SECURE Stopline: structure de signalement anonyme pour les contenus illégaux rencontrés sur Internet
- 15h20-15h40 Présentation de SecurityMadein.LU
- 15h40-16h10 Présentation des activités de prévention et d'accompagnement des entreprises (CASES)
- 16h10-16h30 Pause café
- 16h30-17h30 Présentation des activités et des acteurs dans le domaine de la réaction aux incidents informatiques – CERT.LU, CIRCL, GOVCERT, NCERT.
- 17h30-18h00 Présentation de l'ANSSI (Agence nationale de la sécurité des systèmes d'information)

18h00 Retour des experts à l'hôtel

Jeudi 9 juin 2016

8h30 Départ des experts de l'hôtel

9h00-12h00 Salle de réunion du Ministère de la Justice

- Séance de clôture de la visite (en présence de représentants de tous les acteurs participant à l'évaluation)
- Possibilité, pour les experts, d'approfondir certaines questions

12h00 Fin de la visite

ANNEXE B: LISTE DES PARTICIPANTS

Experts luxembourgeois

a. Coordination

Monsieur Laurent THYES
Ministère de la Justice

Madame Nina BURMEISTER
Service des Médias et des Communications

b. Participants

. Autorités de poursuite

Madame Martine SOLOVIEFF, Parquet général de Luxembourg Monsieur Jeannot NIES, Parquet général de Luxembourg Monsieur Marc HARPES, Parquet général de Luxembourg Madame Dominique PETERS, Parquet de Luxembourg Monsieur Max BRAUN, Parquet de Luxembourg Monsieur Gabriel SEIXAS, Parquet de Luxembourg Monsieur Jim POLFER, Parquet de Luxembourg

. Autorités policières

Monsieur Alain KLEULS
Monsieur Jeff MULLER
Monsieur Michel CONRAD
Monsieur Georges GESCHWINDT
Monsieur Guy VONCKEN
Monsieur Pascal ENZINGER
Monsieur Claude WEIS

. CASES (Cyberworld Awareness and Security Enhancement Services)

Monsieur François THILL

. ANSSI

Monsieur Gérard CAYE

. HCPN

Monsieur Paul RHEIN

. GOVCERT

Monsieur Laurent WEBER

. Security Made In Luxembourg (SMILE)

Monsieur Eric KRIER

Monsieur Pascal STEICHEN

Madame Judith SWIETLIK

Madame Barbara GORGES_WAGNER

Monsieur Georges KNELL

ANNEXE B: LISTE DES ABRÉVIATIONS/GLOSSAIRE DES TERMES UTILISÉS

LISTE DES ACRONYMES, ABRÉVIATIONS ET TERMES UTILISÉS	ACRONYME FRANÇAIS OU DANS LA LANGUE ORIGINALE	NOM COMPLET EN FRANÇAIS OU DANS LA LANGUE ORIGINALE	VERSION ANGLAISE
ANSSI		*Agence nationale de la sécurité des systèmes d'information*	
CIC	*CIC*	*Code d'instruction criminelle*	
CP	*CP*	*Code pénal*	
CRF	*CRF*	*Cellule de renseignement financier*	
CRI	*CRI*	*Commission rogatoire internationale*	
ENISA	*ENISA*	*Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information*	European Union Agency for Network and Information Security
GENVAL	*GENVAL*	*Groupe "Questions générales, y compris l'évaluation"*	Working Party "General Questions including Evaluation"
IP	-	*Internet Protocol*	Internet Protocol
Loi du 17 mars 2014		*Loi modifiée du 17 mars 2004 relative au mandat d'arrêt européen et aux procédures de remise entre États membres de l'Union européenne*	
PGD	*PGD*	*Police grand-ducale*	
SNT	*SNT*	*Section Nouvelles technologies*	
SPJ	*SPJ*	*Service de police judiciaire*	
SREC	*SREC*	*Section de recherche et d'enquêtes criminelles*	

ANNEXE C: LÉGISLATION PERTINENTE

I. Dispositions générales relatives à la responsabilité pénale

Intention, négligence/imprudence	Sauf pour les contraventions et les délits non intentionnels, il faut toujours une intention frauduleuse.
Circonstances aggravantes/atténuantes	Circonstance aggravante générale: **Code pénal: Chapitre V - De la récidive** **"Art. 54** Quiconque, ayant été condamné à une peine criminelle, aura commis un crime emportant la réclusion de cinq à dix ans, pourra être condamné à la réclusion de dix à quinze ans. Si le crime emporte la réclusion de dix à quinze ans, le coupable pourra être condamné à la réclusion de quinze à vingt ans. Il sera condamné à dix-sept ans au moins de cette peine, si le crime emporte la réclusion de quinze à vingt ans. **Art. 56** Quiconque, après une condamnation à une peine criminelle, aura commis un délit, pourra être condamné à une peine double du maximum porté par la loi contre le délit. La même peine pourra être prononcée en cas de condamnation antérieure à un emprisonnement d'un an au moins, si le condamné a commis le nouveau délit avant l'expiration de cinq ans depuis qu'il a subi ou prescrit sa peine. **Art. 57** Les règles établies pour la récidive seront appliquées, conformément aux articles précédents, en cas de condamnation antérieure prononcée par un tribunal militaire, pour un fait qualifié crime ou délit par les lois pénales ordinaires, et à une peine portée par ces mêmes lois. Si, pour ce fait, une peine portée par les lois militaires a été prononcée, les cours et tribunaux, dans l'appréciation de la récidive, n'auront égard qu'au minimum de la peine punie par le premier jugement pouvait entraîner d'après les lois pénales ordinaires. **Art. 57-1** (L. 29 février 2008) 1. Quiconque, ayant été condamné à une peine privative de liberté de plus de cinq ans, par une juridiction d'un Etat membre de l'Union européenne pour des faits visés aux articles 162, 168, 173, 176, 180, tirets 3 à 6, 186, tirets 3 à 6, 192-1 et 192-2, aura commis à nouveau un de ces faits, pourra être condamné à la réclusion de dix ans à quinze

	ans, si ce fait est un crime emportant la réclusion de cinq ans à dix ans. Si ce fait est un crime emportant la réclusion de dix ans à quinze ans, il pourra être condamné à la réclusion de quinze ans à vingt ans. Il sera condamné à la réclusion de dix-sept ans au moins, si ce fait est un crime emportant la réclusion de quinze ans à vingt ans. 2. Quiconque, ayant été condamné à une peine privative de liberté de plus de cinq ans, par une juridiction d'un Etat membre de l'Union européenne pour des faits visés aux articles 162, 163, 168, 169, 170, 173, 176, 177, 180, tirets 3 à 6, 185, 186, tirets 3 à 6, 187-1, 192-1 et 192-2, aura commis à nouveau un de ces faits, pourra être condamné à une peine double du maximum porté par la loi contre ce fait, si ce fait est un délit. 3. Quiconque, ayant été condamné à une peine privative de liberté d'un an au moins, par une juridiction d'un Etat membre de l'Union européenne pour des faits visés aux articles 162, 163, 168, 169, 170, 173, 176, 177, 180, tirets 3 à 6, 185, 186, tirets 3 - 6, 187-1, 192-1 et 192-2, aura, avant l'expiration de cinq ans depuis qu'il a subi ou prescrit sa peine, commis à nouveau un de ces faits, pourra être condamné à une peine double du maximum porté par la loi contre ce fait, si ce fait est un délit. **Art. 57-2** (L. 3 mars 2010) Lorsqu'une personne morale, ayant été condamnée à une peine criminelle au titre de l'article 36, engage sa responsabilité pénale par un nouveau crime, le taux maximum de l'amende applicable est égal au quadruple de celui fixé à l'article 36. Lorsqu'une personne morale, ayant été condamnée à une peine criminelle au titre de l'article 37, engage sa responsabilité pénale par un nouveau crime, le taux maximum de l'amende applicable est égal au quadruple de celui fixé à l'article 37. **Art. 57-3** (L. 3 mars 2010) Lorsqu'une personne morale, ayant été condamnée à une peine criminelle, engage sa responsabilité pénale par un délit, le taux maximum de l'amende applicable est égal au quadruple de celui fixé à l'article 36. Les peines prévues à l'alinéa précédent pourront être prononcées lorsqu'une personne morale, antérieurement condamnée à une amende correctionnelle d'au moins 36.000 euros, engage sa responsabilité par un nouveau délit avant l'expiration de cinq ans depuis qu'elle a subi ou prescrit sa peine." **Code pénal: Chapitre IX - Des circonstances atténuantes**

	(L. 13 juin 1994) **"Art. 73** (L. 13 juin 1994) S'il existe des circonstances atténuantes, les peines criminelles sont réduites ou modifiées conformément aux dispositions qui suivent. **Art. 74** (L. 13 juin 1994) La réclusion à vie est remplacée par la réclusion à temps qui ne peut être inférieure à quinze ans. La réclusion de vingt à trente ans, par la réclusion non inférieure à dix ans. La réclusion de quinze à vingt ans, par la réclusion non inférieure à cinq ans. La réclusion de dix à quinze ans, par la réclusion de cinq à dix ans ou même par un emprisonnement non inférieur à trois ans. La réclusion de cinq à dix ans, par l'emprisonnement de trois mois au moins. **Art. 75** (L. 13 juin 1994) Dans le cas où la loi élève le minimum d'une peine criminelle, le minimum ordinaire de cette peine est appliqué, ou même la peine immédiatement inférieure, conformément à l'article précédent. **Art. 75-1** (L. 3 mars 2010) L'appréciation des circonstances atténuantes dans le chef d'une personne morale s'effectue au regard des peines criminelles encourues par la personne physique pour les faits susceptibles d'engager la responsabilité pénale de la personne morale. **Art. 76** (L. 1er août 2001) L'amende en matière criminelle peut être réduite, sans qu'elle puisse être en aucun cas inférieure à 251 euros. **Art. 77** (L. 1er août 2001) Les coupables dont la peine criminelle a été commuée en un emprisonnement peuvent être condamnés à une amende de 251 euros à 10 000 euros. (L. 13 juin 1994) Ils peuvent être condamnés à l'interdiction de tout ou partie des droits mentionnés à l'article 11, pendant cinq ans au moins et dix ans au plus. **Art. 78** (L. 1er août 2001) S'il existe des circonstances atténuantes, la peine d'emprisonnement peut ne pas être prononcée et l'amende peut être réduite au-dessous de 251 euros, sans qu'elle puisse être inférieure à 25 euros. (L. 13 juin 1994) Si l'interdiction des droits mentionnés à l'article 11 est ordonnée et autorisée, les juges peuvent prononcer ces peines pour un terme d'un an à cinq ans ou les remettre entièrement. **Art. 79** (L. 13 juin 1994) L'appréciation des circonstances atténuantes est réservée aux cours et tribunaux. Ces circonstances sont indiquées dans leurs arrêts et

	jugements."
Conditions d'octroi du sursis	Code d'instruction criminelle: Section IV - Sursis à l'exécution des peines **"Art. 626** (L. 26 juillet 1986) En cas de condamnation contradictoire à une peine privative de liberté et à l'amende, ou à l'une de ces peines seulement, les cours et tribunaux peuvent ordonner, par la même décision motivée, qu'il sera sursis à l'exécution de tout ou partie de la peine. (L. 3 mars 2010) Le sursis est exclu à l'égard des personnes physiques si, avant le fait motivant sa poursuite, le délinquant a été l'objet d'une condamnation devenue irrévocable, à une peine d'emprisonnement correctionnel ou à une peine plus grave du chef d'infraction de droit commun. Le sursis est exclu à l'égard des personnes morales si, avant le fait motivant sa poursuite, le délinquant a été l'objet d'une condamnation devenue irrévocable, à une amende correctionnelle ou à une peine plus grave du chef d'infraction de droit commun. … Section V – Probation **Art. 629** (L. 26 juillet 1986) En cas de condamnation à une peine privative de liberté pour infraction de droit commun, si le condamné n'a pas fait l'objet, pour crime ou délit de droit commun, d'une condamnation antérieure à une peine d'emprisonnement ou s'il n'a été condamné qu'à une peine d'emprisonnement assortie du sursis simple inférieure ou égale à un an, les cours et tribunaux peuvent en ordonnant qu'il sera sursis à l'exécution de tout ou partie de la peine principale pendant un temps qui ne pourra être inférieur à trois années ni supérieur à cinq années, placer le condamné sous le régime du sursis probatoire. Toutefois au cas où la condamnation antérieure aurait déjà été prononcée avec le bénéfice du sursis probatoire, les dispositions du premier alinéa sont inapplicables. Si la condamnation antérieure a été prononcée avec le bénéfice du sursis simple, la première peine n'est exécutée, par dérogation aux dispositions de l'article 627, que si la seconde vient à l'être dans les conditions et délais prévus à l'article 631 ou à l'article 631-2. Cette première peine sera comme non avenue si la seconde peine est considérée comme non avenue dans les conditions et délais prévus à l'article 631-3."

Peine minimale/maximale	Amende de 25 euros/Réclusion à vie
Sanctions alternatives ou cumulatives	**Art. 17** (L. 13 juin 1994) du Code pénal: "Lorsque l'auteur d'un délit encourt une sanction pénale autre que l'emprisonnement ou l'amende, cette sanction peut être prononcée seule à titre de peine principale. **Art. 18** (L. 13 juin 1994) Lorsque l'auteur d'un délit puni de l'emprisonnement a sciemment utilisé, pour préparer ou commettre ce délit, les facilités que lui procure l'exercice d'une activité de nature professionnelle ou sociale, le tribunal peut prononcer à titre de peine principale l'interdiction, pendant une durée de cinq ans au plus, de se livrer à cette activité sous quelque forme et selon quelque modalité que ce soit, sauf s'il s'agit de l'exercice d'un mandat de député ou de conseiller communal. Les dispositions du présent article ne sont pas applicables en matière de délits de presse. **Art. 19** (L. 13 juin 1994) Lorsqu'un délit est puni de l'emprisonnement, la confiscation spéciale telle qu'elle est définie par l'article 31 peut être prononcée à titre de peine principale, alors même qu'elle ne serait pas prévue par la loi particulière dont il est fait application. La disposition de l'alinéa précédent ne s'applique pas en matière de délits de presse. **Art. 20** (L. 13 juin 1994) Lorsqu'un délit est puni de l'emprisonnement et de l'amende, le tribunal peut, à titre de peine principale, ne prononcer que l'une ou l'autre de ces peines. Si l'amende est prononcée seule, elle peut être élevée au double du taux maximum prévu. Si l'emprisonnement est porté seul, le tribunal peut y substituer une amende qui ne peut excéder la somme obtenue par multiplication du maximum de la peine d'emprisonnement prévue, exprimée en jours, par le montant pris en considération en matière de contrainte par corps. **Art. 21** (L. 13 juin 1994) Lorsqu'un délit est puni de l'emprisonnement, le tribunal peut prononcer à titre de peine principale, une ou plusieurs des peines suivantes: 1) interdiction de conduire certains véhicules pendant une durée de cinq ans au plus, ou limitation du droit de conduire pendant la même durée au plus; 2) confiscation d'un ou de plusieurs véhicules dont le prévenu est propriétaire; 3) interdiction de détenir ou de porter, pendant une durée de cinq ans au plus, une arme soumise à autorisation; 4) interdiction du droit d'exercer la chasse pendant une durée de cinq ans au plus;

	5) confiscation d'une ou de plusieurs armes dont le prévenu est propriétaire. **Art. 22** (L. 13 juin 1994) 1) Si de l'appréciation du tribunal, le délit ne comporte pas une peine privative de liberté supérieure à six mois, il peut prescrire, à titre de peine principale, que le condamné accomplira, au profit d'une collectivité publique ou d'un établissement public ou d'une association ou d'une institution hospitalière ou philanthropique, un travail d'intérêt général non rémunéré et d'une durée qui ne peut être inférieure à quarante heures ni supérieure à deux cent quarante heures. 2) Il ne peut être fait application du présent article que lorsque le prévenu est présent. Le président du tribunal, avant le prononcé du jugement, informe le prévenu du droit de refuser l'accomplissement d'un travail d'intérêt général et reçoit sa réponse. 3) L'exécution du travail d'intérêt général doit être commencée dans les dix-huit mois à partir du jour où la décision pénale est devenue irrévocable. 4) Les modalités d'exécution du travail d'intérêt général sont décidées par le procureur général d'Etat. Celui-ci peut notamment suspendre provisoirement pour motif grave d'ordre médical, familial, professionnel ou social, le délai pendant lequel le travail doit être accompli. 5) Un règlement grand-ducal détermine la nature des travaux proposés. 6) Le travail d'intérêt général peut, pour les condamnés salariés, se cumuler avec la durée légale du travail. 7) Les prescriptions légales et réglementaires relatives au travail de nuit, à l'hygiène, à la sécurité, ainsi qu'au travail des femmes et des jeunes travailleurs sont applicables au travail d'intérêt général."

Infractions multiples, récidive	**Code pénal: Chapitre VI - Du concours de plusieurs infractions** **Art. 58** Tout individu convaincu de plusieurs contraventions encourra la peine de chacune d'elles. **Art. 59** En cas de concours d'un ou de plusieurs délits avec une ou plusieurs contraventions, les peines de police seront cumulativement prononcées; la peine correctionnelle la plus forte sera seule prononcée et pourra même être élevée au double du maximum, sans toutefois pouvoir excéder la somme des peines prévues pour les différentes infractions. **Art. 60** En cas de concours de plusieurs délits, la peine la plus forte sera seule prononcée. Cette peine pourra même être élevée au double du maximum, sans toutefois pouvoir excéder la somme des peines prévues pour les différents délits. (L. 13 juin 1994) Toutefois, les peines de substitution seront prononcées cumulativement. **Art. 61** (L. 8 juillet 1996) (1) Lorsqu'un crime concourt, soit avec un ou plusieurs délits, soit avec une ou plusieurs contraventions, la peine la plus forte sera seule prononcée. (2) La peine la plus forte est celle dont la durée de la privation de liberté est la plus longue. (3) Si les peines privatives de liberté sont de même durée, la peine la plus forte est celle dont le taux de l'amende obligatoire est le plus élevé. (4) Si la durée des peines privatives de liberté est la même et que le taux des amendes obligatoires est également le même, la peine la plus forte est celle prévue pour le crime. (5) Dans tous les cas les dispositions concernant la récidive, la prescription, le sursis à l'exécution des peines et la réhabilitation sont celles applicables aux peines criminelles. **Art. 62** En cas de concours de plusieurs crimes, la peine la plus forte sera seule prononcée. Cette peine, si elle consiste dans la réclusion à temps ou dans la réclusion de cinq à dix ans, pourra même être élevée de cinq ans au-dessus du maximum. **Art. 64** Les peines de confiscation spéciale à raison de plusieurs crimes, délits ou contraventions, seront toujours cumulées. **Art. 65** Lorsque le même fait constitue plusieurs infractions, la peine la plus forte sera seule prononcée." Récidive: voir circonstances aggravantes.
Incitation, participation,	**Code pénal: Chapitre VII - De la participation de**

complicité et tentative	**plusieurs personnes au même crime ou délit** **"Art. 66** Seront punis comme auteurs d'un crime ou d'un délit: Ceux qui l'auront exécuté ou qui auront coopéré directement à son exécution; Ceux qui, par un fait quelconque, auront prêté pour l'exécution une aide telle que, sans leur assistance, le crime ou le délit n'eût pu être commis; Ceux qui, par dons, promesses, menaces, abus d'autorité ou de pouvoir, machinations ou artifices coupables, auront directement provoqué à ce crime ou à ce délit; (L. 8 juin 2004) Ceux qui, soit par des discours tenus dans des réunions ou dans des lieux publics, soit par des placards ou affiches, soit par des écrits, imprimés ou non et vendus ou distribués, auront provoqué directement à le commettre, sans préjudice des deux dernières dispositions de l'article 22 de la loi du 8 juin 2004 sur la liberté d'expression dans les médias. **Art. 67** Seront punis comme complices d'un crime ou d'un délit: Ceux qui auront donné des instructions pour le commettre; Ceux qui auront procuré des armes, des instruments ou tout autre moyen qui a servi au crime ou au délit, sachant qu'ils devaient y servir; Ceux qui hors le cas prévu par le paragraphe 3 de l'article 66, auront, avec connaissance, aidé ou assisté l'auteur ou les auteurs du crime ou du délit dans les faits qui l'ont préparé ou facilité, ou dans ceux qui l'ont consommé. **Art. 68** Ceux qui, connaissant la conduite criminelle des malfaiteurs exerçant des brigandages ou des violences contre la sûreté de l'Etat, la paix publique, les personnes ou les propriétés, leur auront fourni habituellement logement, lieu de retraite ou de réunion, seront punis comme leurs complices. **Art. 69** Les complices d'un crime seront punis de la peine immédiatement inférieure à celle qu'ils encourraient s'ils étaient auteurs de ce crime, d'après la graduation prévue par l'article 52 du présent code. La peine prononcée contre les complices d'un délit n'excédera pas les deux tiers de celle qui leur serait appliquée s'ils étaient auteurs de ce délit." **Code pénal: Chapitre IV - De la tentative de crime ou de délit** **"Art. 51** Il y a tentative punissable, lorsque la résolution de commettre un crime ou un délit a été

	manifestée par des actes extérieurs qui forment un commencement d'exécution de ce crime ou de ce délit, et qui n'ont été suspendus ou n'ont manqué leur effet que par des circonstances indépendantes de la volonté de l'auteur. **Art. 52** (L. 7 juillet 2003) La tentative de crime est punie de la peine immédiatement inférieure à celle du crime même. Est considérée comme immédiatement inférieure: a) A la peine de la réclusion à vie, celle de la réclusion de vingt à trente ans; b) A la peine de la réclusion de vingt à trente ans, celle de la réclusion de quinze à vingt ans; c) A la peine de la réclusion de quinze à vingt ans, celle de la réclusion de dix à quinze ans; d) A la peine de la réclusion de dix à quinze ans, celle de la réclusion de cinq à dix ans; e) A la peine de la réclusion de cinq à dix ans, celle d'un emprisonnement de trois mois au moins. **Art. 53** La loi détermine dans quels cas et de quelles peines sont punies les tentatives de délits."
Peines dans le cas d'un procès sommaire ou d'une mise en examen	Pas de peines différentes pour des ordonnances pénales ou un jugement sur accord (procès sommaire)
Autres dispositions générales	/

II. Infractions et sanctions en matière de cybercriminalité

Convention de Budapest **Art. 2 – Accès illégal**	Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.
Disposition correspondante dans le droit interne	**Art. 509-1** (L. 14 août 2000) du Code pénal: "Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement ou de transmission automatisé de données sera puni d'un emprisonnement de deux mois à deux ans et d'une amende de 500 euros à 25 000 euros ou de l'une de ces deux peines. Lorsqu'il en sera résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement sera de quatre mois à deux ans et

	l'amende de 1 250 euros à 25 000 euros."
Intention, négligence/imprudence	Intention frauduleuse nécessaire.
Circonstances aggravantes	Lorsqu'il sera résulté de l'accès frauduleux la suppression ou la modification de données et **Art. 509-4** (L. 10 novembre 2006) du Code pénal: "Lorsque dans les cas visés aux articles 509-1 à 509-3, il y a eu transfert d'argent ou de valeur monétaire, causant ainsi une perte de propriété à un tiers dans un but de procurer un avantage économique à la personne qui commet l'infraction ou à une tierce personne, la peine encourue sera un emprisonnement de quatre mois à cinq ans et une amende de 1 250 euros à 30 000 euros."
Peine minimale/maximale	Emprisonnement de deux mois à cinq ans et amende de 500 euros à 30 000 euros ou une de ces deux peines.

Tentative	**Art. 509-6** (L. 15 juillet 1993) du Code pénal: "La tentative des délits prévus par les articles 509-1 à 509-5 est punie des mêmes peines que le délit lui-même."
Sanctions applicables aux personnes morales	**Code pénal: Chapitre II-1 - Des peines applicables aux personnes morales** (L. 3 mars 2010) **"Art. 34** (L. 3 mars 2010) Lorsqu'un crime ou un délit est commis au nom et dans l'intérêt d'une personne morale par un de ses organes légaux ou par un ou plusieurs de ses dirigeants de droit ou de fait, la personne morale peut être déclarée pénalement responsable et encourir les peines prévues par les articles 35 à 38. La responsabilité pénale des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes infractions. Les alinéas précédents ne sont pas applicables à l'Etat et aux communes. **Art. 35** (L. 3 mars 2010) Les peines criminelles ou correctionnelles encourues par les personnes morales sont: 1) l'amende, dans les conditions et suivant les modalités prévues par l'article 36; 2) la confiscation spéciale; 3) l'exclusion de la participation à des marchés publics; 4) la dissolution, dans les conditions et suivant les modalités prévues par l'article 38. **Art. 36** (L. 3 mars 2010) L'amende en matière criminelle et correctionnelle applicable aux personnes

	morales est de 500 euros au moins. En matière criminelle, le taux maximum de l'amende applicable aux personnes morales est de 750 000 euros. En matière correctionnelle, le taux maximum de l'amende applicable aux personnes morales est égal au double de celui prévu à l'égard des personnes physiques par la loi qui réprime l'infraction. Lorsqu'aucune amende n'est prévue à l'égard des personnes physiques par la loi qui réprime l'infraction, le taux maximum de l'amende applicable aux personnes morales ne peut excéder le double de la somme obtenue par multiplication du maximum de la peine d'emprisonnement prévue, exprimée en jours, par le montant pris en considération en matière de contrainte par corps. **Art. 37** (L. 3 mars 2010) Le taux maximum de l'amende encourue selon les dispositions de l'article 36 est quintuplé lorsque la responsabilité pénale de la personne morale est engagée pour une des infractions suivantes: - crimes et délits contre la sûreté de l'Etat - actes de terrorisme et de financement de terrorisme - infractions aux lois relatives aux armes prohibées en relation avec une association de malfaiteurs ou une organisation criminelle - traite des êtres humains et proxénétisme - trafic de stupéfiants en relation avec une association de malfaiteurs ou une organisation criminelle - blanchiment et recel - concussion, prise illégale d'intérêts, corruption active et passive, corruption privée - aide à l'entrée et au séjour irréguliers en relation avec une association de malfaiteurs ou une organisation criminelle. - (L. 21 décembre 2012) emploi illégal de ressortissants de pays tiers en séjour irrégulier en relation avec une association de malfaiteurs ou une organisation criminelle. **Art. 38** (L. 3 mars 2010) La dissolution peut être prononcée lorsque, intentionnellement, la personne morale a été créée ou, lorsqu'il s'agit d'un crime ou d'un délit puni en ce qui concerne les personnes physiques d'une peine privative de liberté supérieure ou égale à trois ans, détournée de son objet pour commettre les faits incriminés. La dissolution n'est pas applicable aux personnes morales de droit public dont la responsabilité est susceptible d'être engagée. La décision prononçant la dissolution de la personne morale comporte le renvoi de celle-ci devant le tribunal

	compétent pour procéder à la liquidation. **Art. 39** (L. 3 mars 2010) Lorsque la personne morale encourt une peine correctionnelle autre que l'amende, cette peine correctionnelle peut être prononcée seule à titre de peine principale. **Art. 40** (L. 3 mars 2010) Lorsqu'un délit est puni de l'emprisonnement à l'égard des personnes physiques par la loi qui réprime l'infraction, la confiscation spéciale telle qu'elle est définie par l'article 31 peut être prononcée à titre de peine principale à l'égard de la personne morale, alors même qu'elle ne serait pas prévue par la loi particulière dont il est fait application. La disposition de l'alinéa précédent ne s'applique pas en matière de délits de presse."

Observations complémentaires	**Art. 509-7** (L. 15 juillet 1993) du Code pénal: "Quiconque aura participé à une association formée ou à une entente établie en vue de la préparation, concrétisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions prévues par les articles 509-1 à 509-5 sera puni des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée."

i. Sanctions en cas d'interception illégale

Convention de Budapest **Art. 3 – Interception illégale**	Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.
Disposition correspondante dans le droit interne	**Art. 509-3** (L. 14 août 2000) du Code pénal: "[…] sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 1 250 euros à 12 500 euros ou de l'une de ces deux peines. (L. 18 juillet 2014) Sera puni des mêmes peines celui qui aura intentionnellement et au mépris des droits d'autrui, intercepté des données lors de transmissions non publiques à destination, en provenance ou à l'intérieur d'un système de traitement ou de transmission automatisé de données."

Intention, négligence/imprudence	Acte intentionnel et commis au mépris des droits d'autrui.
Circonstances aggravantes	**Art. 509-4** (L. 10 novembre 2006) du Code pénal: "Lorsque dans les cas visés aux articles 509-1 à 509-3, il y a eu transfert d'argent ou de valeur monétaire, causant ainsi une perte de propriété à un tiers dans un but de procurer un avantage économique à la personne qui commet l'infraction ou à une tierce personne, la peine encourue sera un emprisonnement de quatre mois à cinq ans et une amende de 1 250 euros à 30 000 euros."

Peine minimale/maximale	Emprisonnement de trois mois à cinq ans et amende de 1 250 euros à 30 000 euros ou une de ces deux peines.
Tentative	**Art. 509-6** (L. 15 juillet 1993) du Code pénal: "La tentative des délits prévus par les articles 509-1 à 509-5 est punie des mêmes peines que le délit lui-même."
Sanctions applicables aux personnes morales	Cf. ci-dessus
Observations complémentaires	**Art. 509-7** (L. 15 juillet 1993) du Code pénal: "Quiconque aura participé à une association formée ou à une entente établie en vue de la préparation, concrétisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions prévues par les articles 509-1 à 509-5 sera puni des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée."

ii. Sanctions en cas d'atteinte à l'intégrité des données

Convention de Budapest Art. 4 – Atteinte à l'intégrité des données	1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques. 2 Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux.
Disposition correspondante dans le droit interne	**Art. 509-1** (L. 14 août 2000) du Code pénal: "Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement ou de transmission automatisé de données […]. Lorsqu'il en sera résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement sera de quatre mois à deux ans et l'amende de 1 250 euros à 25 000 euros." **Art. 509-3** (L. 14 août 2000) du Code pénal: "Quiconque aura, intentionnellement et au mépris des droits d'autrui, directement ou indirectement, introduit des données dans un système de traitement ou de transmission automatisé ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 1 250 euros à 12 500 euros ou de l'une de ces deux peines. […]"
Intention, négligence/imprudence	Intention frauduleuse/Acte intentionnel et commis au mépris des droits d'autrui.
Circonstances aggravantes	**Art. 509-4** (L. 10 novembre 2006) du Code pénal: "Lorsque dans les cas visés aux articles 509-1 à 509-3, il y a eu transfert d'argent ou de valeur monétaire, causant ainsi une perte de propriété à un tiers dans un but de procurer un avantage économique à la personne qui commet l'infraction ou à une tierce personne, la peine encourue sera un emprisonnement de quatre mois à cinq ans et une amende de 1 250 euros à 30 000 euros.
Peine minimale/maximale	Emprisonnement de trois mois à cinq ans et amende de 1 250 euros à 30 000 euros ou une de ces deux peines.

Tentative	**Art. 509-6** (L. 15 juillet 1993) du Code pénal: "La tentative des délits prévus par les articles 509-1 à 509-5 est punie des mêmes peines que le délit lui-même."
Sanctions applicables aux personnes morales	Cf. ci-dessus
Observations complémentaires	**Art. 509-7** (L. 15 juillet 1993) du Code pénal: "Quiconque aura participé à une association formée ou à une entente établie en vue de la préparation, concrétisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions prévues par les articles 509-1 à 509-5 sera puni des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée."

iii. Sanctions en cas d'atteinte à l'intégrité du système

Convention de Budapest Art. 5 – Atteinte à l'intégrité du système	Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques.
Disposition correspondante dans le droit interne	**Art. 509-2** (L. 15 juillet 1993) du Code pénal: "Quiconque aura, intentionnellement et au mépris des droits d'autrui, entravé ou faussé le fonctionnement d'un système de traitement ou de transmission automatisé de données sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 1 250 euros à 12 500 euros ou de l'une de ces deux peines. **Art. 509-3** (L. 14 août 2000) Quiconque aura, intentionnellement et au mépris des droits d'autrui, directement ou indirectement, introduit des données dans un système de traitement ou de transmission automatisé ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 1 250 euros à 12 500 euros ou de l'une de ces deux peines."

Intention, négligence/imprudence	Acte intentionnel et commis au mépris des droits d'autrui.
Circonstances aggravantes	**Art. 509-4** (L. 10 novembre 2006) du Code pénal: "Lorsque dans les cas visés aux articles 509-1 à 509-3, il y a eu transfert d'argent ou de valeur monétaire, causant ainsi une perte de propriété à un tiers dans un but de procurer un avantage économique à la personne qui commet l'infraction ou à une tierce personne, la peine encourue sera un emprisonnement de quatre mois à cinq ans et une amende de 1 250 euros à 30 000 euros."
Peine minimale/maximale	Emprisonnement de trois mois à cinq ans et amende de 1 250 euros à 30 000 euros.
Tentative	**Art. 509-6** (L. 15 juillet 1993) du Code pénal: "La tentative des délits prévus par les articles 509-1 à 509-5 est punie des mêmes peines que le délit lui-même."
Sanctions applicables aux personnes morales	Cf. ci-dessus
Observations complémentaires	**Art. 509-7** (L. 15 juillet 1993) du Code pénal: "Quiconque aura participé à une association formée ou à une entente établie en vue de la préparation, concrétisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions prévues par les articles 509-1 à 509-5 sera puni des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée."

iv. Sanctions en cas d'abus de dispositifs

Convention de Budapest Art. 6 – Abus de dispositifs	Voir annexe
Disposition correspondante dans le droit interne	**Art. 509-5** (L. 18 juillet 2014) du Code pénal: "Sera puni de 4 mois à cinq ans d'emprisonnement et d'une amende de 1 250 euros à 30 000 euros quiconque aura, dans une intention frauduleuse, produit, vendu, obtenu, détenu, importé, diffusé ou mis à disposition, – un dispositif informatique destiné à commettre l'une des infractions visées aux articles 509-1 à 509-4; ou – toute clef électronique permettant d'accéder, au mépris des droits d'autrui, à tout ou à partie d'un système de traitement ou de transmission automatisé de données."
Intention, négligence/imprudence	Intention frauduleuse nécessaire
Circonstances aggravantes	Non
Peine minimale/maximale	Emprisonnement de quatre mois à cinq ans et amende de 1 250 euros à 30 000 euros.
Tentative	**Art. 509-6** (L. 15 juillet 1993) du Code pénal: "La tentative des délits prévus par les articles 509-1 à 509-5 est punie des mêmes peines que le délit lui-même."
Sanctions applicables aux personnes morales	Cf. ci-dessus
Observations complémentaires	**Art. 509-7** (L. 15 juillet 1993) du Code pénal: "Quiconque aura participé à une association formée ou à une entente établie en vue de la préparation, concrétisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions prévues par les articles 509-1 à 509-5 sera puni des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée."

v. Sanctions en cas de falsification informatique

Convention de Budapest Art. 7 – Falsification informatique	Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.

Disposition correspondante dans le droit interne	**Art. 196** (L. 14 août 2000) du Code pénal: "Seront punies de réclusion de cinq à dix ans les autres personnes qui auront commis un faux en écritures authentiques et publiques, et toutes personnes qui auront commis un faux en écritures de commerce, de banque ou en écritures privées, en ce compris les actes sous seing privé électronique, Soit par fausses signatures, Soit par contrefaçon ou altération d'écritures ou de signatures, Soit par fabrication de conventions, dispositions, obligations ou décharges, ou par leur insertion après coup dans les actes, Soit par addition ou altération de clauses, de déclarations ou de faits que ces actes avaient pour objet de recevoir et de constater. **Art. 197** (L. 14 août 2000) Dans tous les cas exprimés dans la présente section, celui qui aura fait usage du faux sera puni comme s'il était l'auteur du faux. **Art. 488** (L. 14 août 2000) Quiconque aura frauduleusement contrefait ou altéré des clefs, y compris électroniques sera condamné à un emprisonnement de quatre mois à cinq ans et à une amende de 1 250 euros à 30 000 euros. (L. 18 juillet 2014)"
Intention, négligence/imprudence	Intention frauduleuse nécessaire.
Circonstances aggravantes	Non
Peine minimale/maximale	Art. 488: Emprisonnement de quatre mois à cinq ans et amende de 1 250 euros à 30 000 euros, Art. 196 et 197: Réclusion de cinq à dix ans.
Tentative	Art. 488: Non. Art. 196 et 197: Emprisonnement de trois mois au moins.
Sanctions applicables aux personnes morales	Cf. ci-dessus

vi. Sanctions en cas de fraude informatique

Convention de Budapest **Art. 8 – Fraude informatique**	Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui : a par toute introduction, altération, effacement ou suppression de données informatiques ; b par toute forme d'atteinte au fonctionnement d'un système informatique,

	dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.
Disposition correspondante dans le droit interne	**Art. 509-4** (L. 10 novembre 2006) du Code pénal: "Lorsque dans les cas visés aux articles 509-1 à 509-3, il y a eu transfert d'argent ou de valeur monétaire, causant ainsi une perte de propriété à un tiers dans un but de procurer un avantage économique à la personne qui commet l'infraction ou à une tierce personne, la peine encourue sera un emprisonnement de quatre mois à cinq ans et une amende de 1 250 euros à 30 000 euros."
Intention, négligence/imprudence	Intention frauduleuse nécessaire
Circonstances aggravantes	Non
Peine minimale/maximale	Emprisonnement de quatre mois à cinq ans et amende de 1 250 euros à 30 000 euros.
Tentative	**Art. 509-6** (L. 15 juillet 1993) du Code pénal: "La tentative des délits prévus par les articles 509-1 à 509-5 est punie des mêmes peines que le délit lui-même."
Sanctions applicables aux personnes morales	Cf. ci-dessus
Observations complémentaires	**Art. 509-7** (L. 15 juillet 1993) du Code pénal: "Quiconque aura participé à une association formée ou à une entente établie en vue de la préparation, concrétisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions prévues par les articles 509-1 à 509-5 sera puni des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée."

vii. Sanctions en cas d'infraction se rapportant à la pornographie enfantine

Convention de Budapest Art. 9 – Infractions se rapportant à la pornographie enfantine	1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les comportements suivants lorsqu'ils sont commis intentionnellement et sans droit: a la production de pornographie enfantine en vue de sa diffusion par le biais d'un système informatique; b l'offre ou la mise à disposition de pornographie enfantine par le biais d'un système informatique; c la diffusion ou la transmission de pornographie enfantine par le biais d'un système informatique; d le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système informatique ;

	e la possession de pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques. 2 Aux fins du paragraphe 1 ci-dessus, le terme "pornographie enfantine" comprend toute matière pornographique représentant de manière visuelle: a un mineur se livrant à un comportement sexuellement explicite; b une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite; c des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite. 3 Aux fins du paragraphe 2 ci-dessus, le terme "mineur" désigne toute personne âgée de moins de 18 ans. Une Partie peut toutefois exiger une limite d'âge inférieure, qui doit être au minimum de 16 ans. 4 Une Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, les paragraphes 1, alinéas d. et e, et 2, alinéas b. et c.
Disposition correspondante dans le droit interne	**Code pénal Chapitre VII - Des outrages publics aux bonnes mœurs et des dispositions particulières visant à protéger la jeunesse** (L. 16 juillet 2011) **"Art. 383** (L. 16 juillet 2011) Le fait soit de fabriquer, de transporter, de diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humaine, soit de faire commerce d'un tel message, est puni d'un emprisonnement d'un mois à trois ans et d'une amende de 251 à 50 000 euros lorsque ce message est susceptible d'être vu ou perçu par un mineur. **Art. 383bis** (L. 16 juillet 2011) Les faits énoncés à l'article 383 seront punis d'un emprisonnement d'un à cinq ans et d'une amende de 251 à 75 000 euros, s'ils impliquent ou présentent des mineurs ou une personne particulièrement vulnérable, notamment en raison de sa situation administrative illégale ou précaire, d'un état de grossesse, d'une maladie, d'une infirmité ou d'une déficience physique ou mentale. La confiscation des objets prévus à l'article 383 sera toujours prononcée en cas de condamnation, même si la propriété n'en appartient pas au condamné ou si la condamnation est prononcée par le juge de police par l'admission de circonstances atténuantes. **Art. 383ter** (L. 16 juillet 2011) Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni d'un d'emprisonnement d'un mois à trois ans et d'une amende de 251 à 50 000 euros. Le fait d'offrir, de rendre disponible ou de diffuser une

	telle image ou représentation, par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter, est puni des mêmes peines. Les faits seront punis d'un emprisonnement d'un à cinq ans et d'une amende de 251 à 100 000 euros lorsqu'il a été utilisé, pour la diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé, un réseau de communications électroniques. La tentative des délits prévus aux alinéas précédents est punie des mêmes peines. **Art. 384** (L. 21 février 2013) Sera puni d'un emprisonnement d'un mois à trois ans et d'une amende de 251 à 50 000 euros, quiconque aura sciemment acquis, détenu ou consulté des écrits, imprimés, images, photographies, films ou autres objets à caractère pornographique impliquant ou présentant des mineurs. (L. 16 juillet 2011) La confiscation de ces objets sera toujours prononcée en cas de condamnation, même si la propriété n'en appartient pas au condamné ou si la condamnation est prononcée par le juge de police par l'admission de circonstances atténuantes. **Art. 385** (L. 31 mai 1999) Quiconque aura publiquement outragé les mœurs par des actions qui blessent la pudeur, sera puni d'un emprisonnement de huit jours à trois ans et d'une amende de 251 euros à 25 000 euros. **Art. 385-1** (L. 8 juin 2004) Quiconque aura publiquement outragé les mœurs par des chansons, pamphlets, figures, écrits, imprimés, dessins, gravures, peintures, emblèmes, images ou par tout autre support de l'écrit, du son, de la parole ou de l'image communiqués au public par la voie d'un média, sera puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 12 500 euros. **Art. 385-2** (L. 16 juillet 2011) Le fait pour un majeur de faire des propositions sexuelles à un mineur de moins de seize ans ou à une personne se présentant comme telle en utilisant un moyen de communication électronique est puni d'un emprisonnement d'un mois à trois ans et d'une amende de 251 à 50 000 euros. Il sera puni d'un emprisonnement d'un à cinq ans et d'une amende de 251 à 75 000 euros lorsque les propositions ont été suivies d'une rencontre. **Art. 385bis** (L. 31 mai 1999) Sera puni d'une amende de 251 euros à 25 000 euros quiconque vend ou distribue à des enfants de moins de seize ans des écrits, images, figures ou objets indécents de nature à troubler leur imagination. Sera puni de la même peine quiconque expose publiquement dans le voisinage d'un établissement

	d'instruction ou d'éducation fréquenté par des enfants de moins de seize ans des écrits, images, figures ou objets indécents de nature à troubler leur imagination. La confiscation des écrits, figures ou objets indécents exposés, mis en vente ou en distribution sera toujours prononcée en cas de condamnation, même si la propriété n'en appartient pas au condamné ou si la condamnation est prononcée par le juge de police par l'admission de circonstances atténuantes. **Art. 386** Dans les cas prévus au présent chapitre, les coupables pourront, de plus, être condamnés à l'interdiction des droits indiqués aux numéros 1, 3, 4, 5 et 7 de l'article 11. (L. 21 février 2013) Ils pourront également être condamnés à l'interdiction pour une durée de dix ansau plus, d'exercer une activité professionnelle, bénévole ou sociale impliquant un contact habituel avec des mineurs. Toute violation de cette interdiction est punie d'un emprisonnement de deux mois à deux ans."
Intention, négligence/imprudence	Intention frauduleuse nécessaire.
Circonstances aggravantes	Voir le texte des articles.
Peine minimale/maximale	Emprisonnement d'un mois à cinq ans et amende de 251 euros à 100 000 euros
Tentative	Art. 383ter du Code pénal: Oui. Mêmes peines. Pour les autres articles concernés: Non.
Sanctions applicables aux personnes morales	Cf. ci-dessus
Observations complémentaires	Sans objet

viii. Sanctions en cas d'infraction liée aux atteintes à la propriété intellectuelle et aux droits connexes

Convention de Budapest **Art. 10 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes**	1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes à la propriété intellectuelle, définies par la législation de ladite Partie, conformément aux obligations que celle-ci a souscrites en application de l'Acte de Paris du 24 juillet 1971 portant révision de la Convention de Berne pour la protection des œuvres littéraires et artistiques, de l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et du traité de l'OMPI sur la propriété intellectuelle, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique. 2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en

	infraction pénale, conformément à son droit interne, les atteintes aux droits connexes définis par la législation de ladite Partie, conformément aux obligations que cette dernière a souscrites en application de la Convention internationale pour la protection des artistes interprètes ou exécutants, des producteurs de phonogrammes et des organismes de radiodiffusion (Convention de Rome), de l'Accord relatif aux aspects commerciaux des droits de propriété intellectuelle et du Traité de l'OMPI sur les interprétations et exécutions, et les phonogrammes, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique. 3 Une Partie peut, dans des circonstances bien délimitées, se réserver le droit de ne pas imposer de responsabilité pénale au titre des paragraphes 1 et 2 du présent article, à condition que d'autres recours efficaces soient disponibles et qu'une telle réserve ne porte pas atteinte aux obligations internationales incombant à cette Partie en application des instruments internationaux mentionnés aux paragraphes 1 et 2 du présent article.
Disposition correspondante dans le droit interne	**Loi modifiée du 18 avril 2001 sur les droits d'auteur, les droits voisins et les bases de données** **"Sanctions pénales** **Art. 82** Toute atteinte méchante ou frauduleuse portée aux droits protégés au titre de la présente loi de l'auteur, des titulaires de droits voisins et des producteurs de bases de données constitue le délit de contrefaçon. Est coupable du même délit, quiconque, sciemment, vend, offre en vente, importe, exporte, fixe, reproduit, communique, transmet par fil ou sans fil, met à la disposition du public et de manière générale, met ou remet en circulation, à titre onéreux ou gratuit, une oeuvre, une prestation ou une base de données sans autorisation de l'auteur, du titulaire des droits voisins ou du producteur de base de données. Est ainsi notamment coupable de ce délit, quiconque, sciemment, met à la disposition du public des phonogrammes, vidéogrammes, CD-ROM, multimédias ou tous autres supports, programmes ou bases de données réalisés sans l'autorisation des titulaires de droits d'auteur ou de droits voisins ou des producteurs de bases de données, ainsi que ceux qui reproduisent des œuvres, des prestations ou des bases de données protégées pour les numériser, les mémoriser, les stocker, les distribuer, les injecter, et de façon générale, rendre possible leur accès par le public,

	ou leur communication au public. **Art. 83** Les délits prévus à l'article précédent seront punis d'une amende de 251 euros à 250 000 euros. La confiscation des ouvrages ou objets contrefaisants ou des supports contenant les contrefaçons, de même que celle des planches, moules ou matrices et autres ustensiles ayant directement servi à commettre les délits visés à l'article précédent, sans condition quant à leur propriété, sera prononcée contre les condamnés, ainsi que celle de leur matériel de copiage, de numérisation ou d'injection sur les réseaux. Le jugement pourra de même ordonner la destruction des choses confisquées. **Art. 84** L'application méchante ou frauduleuse sur une œuvre ou une base de données protégée du nom d'un auteur ou d'un titulaire de droits voisins ou d'un droit sui generis du producteur de base de données ou de tout autre signe distinctif adopté par lui pour désigner son œuvre, sa prestation ou sa production sera punie d'un emprisonnement de 3 mois à 2 ans et d'une amende de 251 euros à 250 000 euros ou de l'une de ces peines seulement. Il en est de même pour l'application méchante ou frauduleuse à l'occasion de l'exploitation de la prestation d'un titulaire de droits voisins ou d'un producteur de bases de données ou sur le support qui contient cette prestation du nom d'un titulaire de droits voisins ou d'un droit "sui generis" des producteurs de bases de données ou de tout autre signe distinctif adopté par lui. La confiscation des objets contrefaits sera prononcée dans tous les cas. Le juge pourra de même ordonner leur destruction. Ceux qui, sciemment, vendent, offrent en vente, importent, exportent, fixent, reproduisent, communiquent, transmettent par fil ou sans fil, mettent à la disposition du public et de manière générale, mettent ou remettent en circulation à titre onéreux ou gratuit, les objets ou prestations désignés au premier alinéa du présent article seront punis des mêmes peines. **Art. 85** Toute récidive relative aux délits prévus aux articles précédents est punie d'un emprisonnement de 3 mois à 2 ans et d'une amende de 500 euros à 500 000 euros, ou de l'une de ces peines seulement. En outre, le tribunal peut ordonner, soit à titre définitif, soit à titre temporaire pendant la durée qu'il précise, la fermeture de l'établissement exploité par le condamné pour une durée qui ne dépassera pas 5 ans. Il peut également ordonner, aux frais du condamné, la publication et l'affichage du jugement prononçant la condamnation. **Art. 86** Les personnes morales sont solidairement

	tenues responsables des condamnations, dommages et intérêts, amendes, frais, confiscations, restitutions et sanctions pécuniaires et en nature, prononcées pour infraction aux dispositions de la présente loi contre leurs administrateurs, représentants et préposés."
Intention, négligence/imprudence	Intention frauduleuse nécessaire.
Circonstances aggravantes	Voir article 85 ci-dessus sur la récidive.
Peine minimale/maximale	Amende de 251 euros/Emprisonnement de deux ans.
Tentative	Non
Sanctions applicables aux personnes morales	Cf. ci-dessus et article 86 ci-dessus.
Observations complémentaires	Sans objet