

**Objet: Projet de loi n°6514 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. (4069SBE)**

*Saisine : Ministre de la Justice  
(12 décembre 2012)*

## **AVIS DE LA CHAMBRE DE COMMERCE**

L'objet du projet de loi sous avis est de **renforcer la lutte contre la cybercriminalité**, c'est-à-dire les actes de délinquance commis à l'aide des nouvelles technologies, (i) en ratifiant la Convention du Conseil de l'Europe sur la cybercriminalité du 23 novembre 2001 ainsi que son Protocole additionnel du 28 janvier 2003 relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques et (ii) en apportant les changements nécessaires à la législation luxembourgeoise pour la mettre en conformité avec la Convention et son Protocole additionnel.

La Convention du Conseil de l'Europe sur la cybercriminalité est un instrument juridique exhaustif qui couvre tous les aspects importants de la lutte contre la cybercriminalité en établissant une terminologie, en harmonisant les éléments d'infractions prévus par le droit pénal matériel, en fournissant au droit procédural les moyens nécessaires à la poursuite des infractions et en mettant en place un régime rapide de coopération internationale. Quant au Protocole additionnel, sa raison d'être s'explique par la nécessité de combattre sur un plan international les actes de racisme et de xénophobie commis par le biais de systèmes informatiques.

### **Considérations générales**

La Chambre de Commerce salue le projet de loi sous avis qui contribue sensiblement au renforcement de la lutte contre la cybercriminalité au Luxembourg mais également à l'échelle internationale, avec l'approbation de la Convention du Conseil de l'Europe sur la cybercriminalité ainsi que son Protocole additionnel. Elle soutient en effet l'idée que le caractère transfrontalier de la cybercriminalité nécessite la mise en place, à travers des instruments internationaux, de mesures de protection des systèmes informatiques mais également de mesures juridiques de prévention et de dissuasion, afin de sécuriser le recours aux technologies de l'information au premier rang desquelles figure internet.

La Chambre de Commerce rappelle à cette occasion la récente ouverture, le 11 janvier 2013, du Centre européen de lutte contre la cybercriminalité<sup>1</sup> - dont l'objectif est de renforcer la protection des entreprises dans l'Union européenne - qui atteste de la prise de conscience par les Etats de l'importance du phénomène que constitue la cybercriminalité et de la nécessité de le combattre à l'échelle internationale.

Plus généralement, la Chambre de Commerce relève que le projet de loi sous avis tend, à l'instar des projets de loi portant sur la possibilité de revendiquer des données informatiques en cas de faillite<sup>2</sup> et l'archivage électronique<sup>3</sup>, à renforcer le cadre législatif luxembourgeois de l'économie numérique et partant la crédibilité du Luxembourg dans ce secteur en pleine expansion.

Pour toutes ces raisons, et en dépit de la ratification tardive de la Convention et de son Protocole additionnel par le Luxembourg, la Chambre de Commerce ne peut que soutenir le présent projet de loi et saluer le travail des auteurs pour la pertinence des dispositions introduites dans la législation luxembourgeoise, en particulier sur les points suivants :

**La cohérence du droit pénal est préservée** grâce au choix des auteurs :

- de n'avoir pas opté pour une loi spécifique sur la cybercriminalité - au motif que la législation luxembourgeoise actuelle couvre la majeure partie des articles de la Convention - mais plutôt d'avoir procédé, dans le Code pénal et le Code d'instruction criminelle, à l'insertion des nouvelles infractions incriminées par la Convention<sup>4</sup> ;
- d'avoir harmonisé le seuil minimal de la peine d'emprisonnement éventuellement encourue en cas d'infractions informatiques, en le relevant d'un à quatre mois.

**La sécurité juridique est renforcée** puisque :

- l'infraction d'*usurpation d'identité*, actuellement limitée au port public de faux nom patronymique, sera élargie au cas d'usurpation faite dans un cadre non public de nom (nom de société) ou d'une identification de quelque nature qu'elle soit (certificat Luxtrust, matricule de sécurité sociale...), ce qui devient indispensable notamment en matière de signature électronique ;
- la technique de l'*hameçonnage* (ou *phishing*) utilisée par des fraudeurs pour obtenir des renseignements personnels (tels que mot de passe, numéro de compte ou de carte bancaire) par le biais de courriers électroniques, de sites web falsifiés ou tous autres moyens électroniques, sera à l'avenir appréhendée par le droit pénal. Cette nouvelle incrimination répond à un arrêt de la Cour d'appel du 14 juin 2010 qui avait considéré que dans sa rédaction actuelle, l'article 496 du Code pénal ne permettait pas de retenir l'escroquerie en cas d'hameçonnage d'un mot de passe ;
- outre les nouvelles infractions précitées, seront insérées dans le Code pénal l'*interception ou tentative d'interception de données informatiques* (lors de transmissions non publiques à destination, en provenance ou à l'intérieur d'un système de traitement ou de transmission automatisé de données) ainsi que l'*abus de dispositif* (qui a pour but de prohiber la fabrication, la possession et la diffusion de programmes informatiques permettant de commettre des infractions pénales, ainsi que le trafic des mots de passe ou des codes d'accès).

---

<sup>1</sup> Site officiel : « [www.europol.europa.eu/ec3](http://www.europol.europa.eu/ec3) ».

<sup>2</sup> Projet de loi n°6485 portant modification de l'article 567 du Code de commerce.

<sup>3</sup> Projet de loi n°6543 relatif à l'archivage électronique et modifiant la loi modifiée du 5 avril 1993 relative au secteur financier.

<sup>4</sup> Concernant les dispositions contenues dans le Protocole additionnel, elles sont couvertes par les dispositions législatives actuellement en vigueur,

**La lutte contre le blanchiment et le financement du terrorisme est renforcée grâce au fait que les infractions informatiques sont érigées en infractions primaires :**

- Alors qu'actuellement, certaines infractions informatiques génératrices de revenus importants échappent soit à toute poursuite – à défaut d'être incriminées – soit ne sont pas qualifiées d'infractions primaires et ne peuvent dès lors pas donner lieu à des poursuites au titre du blanchiment, il sera possible à l'avenir de poursuivre l'infraction de blanchiment en cas d'utilisation des revenus tirés des infractions informatiques.
- Le projet de loi s'inscrit à cet égard en conformité avec les nouvelles recommandations du GAFI et de la proposition de 4<sup>ème</sup> directive de lutte contre le blanchiment et le financement du terrorisme, ce dont la Chambre de Commerce se félicite.

**Le droit procédural se dote de véritables moyens de lutte contre les infractions informatiques** puisque :

- le juge d'instruction pourra (i) procéder au repérage des données d'appel de moyens de télécommunication et de pouvoir localiser l'origine ou la destination de télécommunications sans qu'une instruction préparatoire ne soit ouverte ; et (ii) enjoindre une personne ayant des connaissances particulières du système informatique ou du mécanisme de protection ou de cryptage, hormis celle visée par l'instruction, à lui donner accès aux données saisies (injonction de produire),
- les officiers de police judiciaire pourront (i) procéder à des perquisitions et saisies des données informatiques stockées en la possession des personnes incriminées ; et (ii) faire procéder à la conservation rapide et immédiate, pendant un délai qui ne peut excéder 90 jours, des données stockées, traitées ou transmises dans un système informatique lorsqu'il y a des raisons de penser que ces données sont susceptibles de perte ou de modification.

## Commentaires des articles

### Concernant l'article 3

Sous **le point 5)** de l'article 3 du projet de loi qui modifie le point 1) de l'article 506-1 du Code pénal - relatif à l'infraction de blanchiment -, la Chambre de Commerce s'étonne qu'au dix-septième tiret, la référence à *l'article 143 de la loi modifiée du 29 août 2008 portant sur la libre circulation des personnes et l'immigration* ait été ajoutée dans la mesure où cet article 143 a été abrogé par la loi du 21 juillet 2012 portant : 1) approbation du Protocole contre le trafic illicite de migrants par terre, air et mer, signé à Palerme, le 12 décembre 2000, additionnel à la Convention des Nations Unies contre la criminalité transnationale organisée le 15 novembre 2000, 2) modification du Code pénal, 3) modification du Code d'instruction criminelle, 4) modification de la loi modifiée du 29 août 2008 portant sur la libre circulation des personnes et l'immigration.

Parallèlement, la Chambre de Commerce ne comprend pas pourquoi dans le nouvel article 506-1 du Code pénal proposé par le présent projet de loi, la référence aux *articles 382-4 et 382-5 du Code pénal* a été supprimée alors que ces deux articles ont été insérés par la loi du 21 juillet 2012 précitée, suite à l'abrogation de l'article 143 de la loi modifiée du 29 août 2008 portant sur la libre circulation des personnes et l'immigration, pour former le « Chapitre VI-II. - Du trafic illicite des migrants ». Il convient partant de remédier à ces erreurs de renvoi.

Le **point 8)** de l'article 3 du projet de loi introduit un article 509-5 dans le Code pénal réprimant spécifiquement *la production, la vente, l'obtention, la détention, l'importation, la diffusion ou la mise à disposition de dispositif informatique permettant de commettre des infractions informatiques ou d'obtenir un mot de passe ou code d'accès.*

A la lecture du commentaire des articles, la Chambre de Commerce comprend que cette nouvelle disposition remplacera l'alinéa 2 à l'article 509-3 du Code pénal - corrélativement supprimé par le point 7) de l'article 3 du projet de loi - qui réprime *la fabrication, la réception, l'obtention, la détention, la vente ou la cession à des tiers des logiciels permettant de commettre des infractions informatiques*. Dans ce contexte, la Chambre de Commerce s'étonne, à défaut pour les auteurs d'en justifier les raisons, de l'abaissement de l'amende prévue à l'alinéa 2 à l'article 509-3 du Code pénal, actuellement de 1.250 euros à 30.000 euros, et de son remplacement par une amende de 251 euros à 5.000 euros seulement.

\* \* \*

Après consultation de ses ressortissants, la Chambre de Commerce est en mesure d'approuver le présent projet de loi sous avis.

SBE/TSA