

Stopper les cybercriminels

Pour plus de sécurité, adoptez les réflexes CASES !

Porter plainte – à quoi faut-il faire attention ?

Qu'il s'agisse d'intrusion sur des systèmes ou de manipulation de données, les malfaiteurs doivent s'attendre à des poursuites tant que le plan pénal que civil. Le Luxembourg dispose d'une jurisprudence claire, mais seules les infractions qui font l'objet d'une plainte peuvent donner lieu à des poursuites légales. Les victimes d'un délit criminel doivent donc conserver des preuves et ne pas avoir peur de le dénoncer.

Les suggestions appétissantes du site Internet d'un restaurant ont soudainement été remplacées par des images pornographiques. Le blog d'une écolière contient un matin des contenus offensants dirigés contre la fillette. Le collaborateur d'une organisation a sciemment changé les mots de passe pour compliquer l'accès aux données. Par vengeance, quelqu'un envoie un virus par e-mail. Des parents surfent sur Internet et se retrouvent face à des contenus racistes. Une entreprise remarque une intrusion sur l'infrastructure du système. Un enfant est victime de harcèlement sexuel sur un chat.

Des lois ont-elles été enfreintes dans les cas cités ? S'agit-il d'une liste de délits ? De délits mineurs ? Méritent-ils une plainte ? Une plainte n'entraînerait-elle pas encore plus de dommages pour la victime ? Les exemples cités montrent-ils la face plus sombre de notre monde informatisé qui doit être acceptée comme le prix à payer pour avoir accès aux connaissances ? Ces questions reflètent les opinions et points de vue les plus divers des participants aux nombreuses formations et conférences du portail de la sécurité de l'information CASES.



Le Luxembourg a des lois claires qui s'appliquent aussi au monde numérique.

Mais, sans plaignant, un juge ne peut pas statuer. Les exemples ci-dessus représentent des infractions à la loi. Toutefois, en l'absence de plainte ou de signalement de tels délits, les pirates ne pourront pas être retrouvés et les menaces ne pourront pas être évitées à temps.

Le non-respect fréquent des normes et lois sociales sans mesure ou sanction peut en outre entraîner l'essor des activités criminelles et une dilution de notre sens de la justice sociale. Prenons un exemple pour l'illustrer. Prendre des produits dans un supermarché sans les payer est interdit par la loi. Il s'agit de vol. S'il y a larcin, il y aura plainte ou le voleur sera sanctionné. Que se passerait-il si les personnes qui se servent n'encouraient ni amende ni sanction ? Les vols dans les magasins seraient certainement bien plus nombreux qu'actuellement.

Nos fondements légaux valent aussi pour le monde numérique. Les

infractions doivent donc, comme dans le monde réel, faire l'objet d'une plainte. Les criminels pourront ainsi être arrêtés et les éventuelles menaces évitées.

Les règles luxembourgeoises du Code pénal

Quiconque fait preuve de discrimination ou de racisme sur des supports numériques doit s'attendre à des sanctions conformément à l'article 454 du Code pénal luxembourgeois. Cet article intervient aussi lorsque quelqu'un tente de mettre en doute ou de réinterpréter des faits historiques, politiques ou scientifiques établis.

Toute tentative de s'approprier une propriété étrangère sous un faux nom sera punie par l'article 496. Ainsi, quiconque tentera d'escroquer quelqu'un via une fausse identité numérique contrevient clairement à la loi.

Les calomnies, diffamations ou propos injurieux sont sanctionnés par les articles 443 et suivants, 448 et 561-7. Une calomnie publiée sur un

site Internet ou un SMS insultant constitue donc une infraction à la loi et peut être sanctionné.

La diffusion de matériel pornographique à des enfants de moins de seize ans est interdite par l'article 385bis du Code pénal. Par conséquent, toute personne qui envoie une photo ou vidéo pornographique à un jeune de moins de 16 ans se rend coupable d'un délit. Pour les contenus à caractère pédophile, l'article 384 du Code pénal luxembourgeois intervient.

Les abus de confiance sont régis par les articles 491 à 493 et les infractions en matière informatique par les articles 509-1 à 509-7. Ce dernier article précise les responsabilités civiles et pénales d'un criminel et les sanctions qu'il encourt.

Sanctions en cas d'infractions dans le domaine informatique

Accéder illégalement à un système qui traite ou transmet automatiquement des données est répréhensible. Cette intrusion peut se faire via un ordinateur de l'organisation ou de l'entreprise, ou à distance.

La sanction prévue par l'article 509-1 du Code pénal luxembourgeois pour un tel accès illégal peut aller jusqu'à deux ans de prison et une amende de 500 à 25 000 euros. L'utilisation d'un logiciel permettant, par exemple, d'accéder à des téléphones mobiles étrangers constitue un accès illégal. Un logiciel appelé Superbluetooth est très apprécié des jeunes luxembourgeois. Accéder à un téléphone étranger n'est cependant ni amusant ni un délit mineur, il s'agit d'une infraction pénale.

La destruction ou la modification intentionnelle de données est également punissable. Toute personne s'introduisant illégalement dans un système doit s'attendre à une peine de prison de 4 à 24 mois et à une amende de 1250 à 25 000 euros conformément à l'article 509-2. La destruction ou la modification intentionnelle de données sans accès illégal est bien entendu également punissable. On pense ici, par exemple, à des sentiments de vengeance d'un employé. Selon l'article 509-3, la sanction va de 3 à 36 mois d'emprisonnement et de 1250 à 12 500 euros d'amende.

L'article 509 prévoit en outre une sanction en cas de blocage intentionnel ou de destruction volontaire d'un système. Sont aussi répréhensibles les manipulations de logiciels ou de matériel qui entraînent des dysfonctionnements ou une perte de performance du système.

Même les tentatives d'attaque sont punissables, qu'elles aboutissent ou non. Les mêmes sanctions s'appliquent qu'en cas d'infraction. Le regroupement de plusieurs personnes ou leur accord pour perpétrer une attaque est sanctionné par l'article 509-7. Ici aussi, les mêmes sanctions s'appliquent qu'en cas d'infraction.

De surcroît, la personne peut être poursuivie sur le plan civil. Une

victime, entreprise ou particulier, peut réclamer des dommages-intérêts à l'auteur de l'attaque en vertu de l'article 1382 du Code civil.

Porter plainte – à quoi faut-il faire attention ?

La plainte doit être déposée aussi rapidement que possible. Elle doit aussi être très bien préparée. Les chances de réussite d'une action sont d'autant plus grandes que l'utilisateur concerné ou l'organisation attaquée peut fournir un maximum de données.

Il est donc important de conserver des preuves des faits correspondants. Si, par exemple, une entreprise fait appel à une société de sécurité de l'information pour réparer les

Conseil de sécurité : sauvegarder les preuves, signaler les contenus illégaux

Il arrive souvent que les preuves ne soient pas sauvegardées ou soient même effacées, par exemple en cas de harcèlement sexuel, de calomnie ou de sites Internet ayant des contenus illégaux, par exemple des contenus racistes. Or, les preuves sont capitales dans le cas d'une plainte ou d'une action en justice. La preuve des faits doit donc être conservée impérativement.

L'utilisateur doit enregistrer les contenus apparaissant à l'écran à titre de preuve. Pour cela, il suffit d'appuyer simultanément sur les touches « Alt » et « Imprimer », ce qui permet de capturer la fenêtre du navigateur. Il faut ensuite ouvrir Word ou un programme graphique pour insérer et enregistrer la preuve en appuyant simultanément sur les touches « Ctrl » et « V ». Attention ensuite à ne pas oublier de sauvegarder, par exemple avec la touche « F12 ».

Dans les chats, les parties de texte problématiques peuvent être surlignées avec la souris et copiées en appuyant en même temps sur les touches « Ctrl » et « C ». Il suffit ensuite d'ouvrir Word pour insérer le texte en appuyant simultanément sur les touches « Ctrl » et « V ». Ici aussi, ne pas oublier d'enregistrer !

Les applications comme MSN, surtout utilisées par les enfants pour bavarder par ordinateur interposé, offrent en outre une fonction qui sauvegarde automatiquement tous les contenus. Il est toutefois recommandé aux parents de ne pas utiliser cette fonction pour surveiller leurs enfants mais de parler avec eux et de leur expliquer le caractère protecteur de cette fonction.

Il est conseillé aux utilisateurs de signaler tout contenu illégal qu'ils rencontrent sur Internet. C'est la seule solution pour arrêter les malfaiteurs. Cette opération peut aussi se faire anonymement via <http://www.lisa-stopline.lu> ou la ligne téléphonique 8002-6767.

Définition : navigateur

Un navigateur est un programme informatique spécial pour visualiser les pages web d'Internet.

Définition : chat

Un chat est un espace virtuel personnel où les utilisateurs peuvent communiquer entre eux en temps réel. Beaucoup de jeunes aiment « chatter » par ordinateur. Traduit de l'anglais, « to chat » ne signifie rien d'autre que « bavarder ».

dommages, comme restaurer des données, un rapport détaillé doit être établi. Il pourra être très utile en cas d'action en justice et de réclamation de dommages-intérêts.

Si on tombe sur des sites publiant des contenus illégaux, à caractère raciste ou pédophile, par exemple, il faut noter le nom du site ainsi que la date et l'heure. Le fait doit être décrit aussi précisément que possible et

enregistré. Cela vaut aussi pour les autres infractions à la loi comme la calomnie ou la diffamation. Il ne faut en aucun cas effacer les données. Ceci est d'ailleurs également vrai pour les e-mails.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu