Quelle lutte contre la cybercriminalité en Europe ?

Manger, s'habiller, regarder des films, écouter de la musique, préparer ses vacances... Tout cela est possible grâce à Internet. Ce jeune média, né au début des années 90, a vu son utilisation augmenter de façon fulgurante. Le revers de la médaille : la cybercriminalité. Voici le premier article d'une prochaine série consacrée à ce thème.

« Découvrez comment gagner 1 000 € en restant sur votre canapé ! ». « Veuillez renseigner vos coordonnées bancaires pour obtenir un bonus de 10 000 € ». Vous avez déjà reçu ce genre d'emails ? Vous avez fait l'objet d'une cyberattaque, de cybercriminalité. Cette nouvelle menace du XXIème siècle frappe de plus en plus de personnes, 13,7 millions de personnes ont été confrontées à la cybercriminalité en France en 2016. Elle ne prend pas seulement en compte les arnaques bancaires mais aussi l'apologie du terrorisme, les réseaux de pédopornographie ou de proxénétisme; les attaques contre des systèmes de données et les escroqueries bancaires.

Les particuliers ne sont pas les seules personnes concernées. Orange, Uber, Dominos Pizza, Paypal, la SNCF et d'autres entreprises ont également été touchées par des attaques cybercriminelles. Les Etats, eux-aussi, ne sont pas à l'abri du danger. Vendredi 9 février, lors de l'ouverture des Jeux Olympiques d'Hiver à Pyeongchang, le site internet de l'événement a été complètement paralysé empêchant les utilisateurs d'imprimer leurs tickets. A tout moment les données des utilisateurs d'internet peuvent faire l'objet de vol et de piratage. Mieux vaut réfléchir à deux fois avant d'enregistrer son numéro de carte bleu sur Internet.

Le principe d'Internet étant de pouvoir communiquer partout dans le monde, la spécificité de la cybercriminalité est qu'elle attaque au-delà des frontières. Ce qui rend la résolution de ces conflits difficiles pour un Etat, seul. En effet comment faire pour retrouver le cybercriminel ? Comment mettre en place son arrestation ? Quelle peine lui infliger ?

La coopération entre les Etats est donc de mise dans ce genre d'affaires. Plusieurs outils existent. Au niveau international, Interpol s'occupe de neutraliser les réseaux cybercriminels. Dans l'Union européenne, Europol a inauguré en 2013 le Centre européen de lutte contre la cybercriminalité ou EC3. Son rôle est de notifier aux Etats membres les principales menaces de la cybercriminalité, sur leurs défaillances en matière de défense en ligne, d'identifier et trouver les réseaux organisés de criminels, de fournir un appui opérationnel à l'enquête.

Par ailleurs, le mandat d'arrêt européen, dont avait fait objet Salah Abdeslam accusé d'avoir participé aux attentats du 13 Novembre 2017 en France, permet d'accélérer les procédures d'arrestation. Ce qui se révèle très utile quand des réseaux de cybercriminalité sont découverts en Europe. Plus rapide que la procédure d'extradition, le mandat d'arrêt européen permet de transférer un suspect dans l'Etat où les faits sont reprochés entre 10 et 50 jours. Cette coopération judiciaire entre les Etats membres de l'Union européenne n'implique que les juges et non les gouvernements, contrairement à l'extradition.

Mais un autre problème persiste. Une fois la personne arrêtée, il faut pouvoir être en mesure de définir son infraction. La cybercriminalité a besoin d'être encadrée par des lois et autres textes juridiques. Or, les Etats peuvent avoir des législations différentes sur la question. L'outil juridique qui harmonise les lois nationales est la Convention de Budapest sur la cybercriminalité du Conseil de l'Europe. C'est le premier traité international qui définit les infractions pénales commises via Internet et d'autres réseaux informatiques concernant les droits d'auteur, la fraude informatique et la pornographie enfantine. Son objectif est de mettre en œuvre une politique pénale commune destinée à protéger la société de la criminalité dans le cyberespace. Actuellement, la Convention de Budapest est signée par 67 Etats dont certains se trouvent bien au-delà des frontières européennes avec les Etats-Unis, le Japon et le Panama. La complexité de la cybercriminalité oblige les Etats à définir sans cesse de nouveaux moyens d'action.

La cybercriminalité recouvre un champ très vaste de problématiques. Elle reste encore difficile à appréhender. Certains considèrent les Anonymous comme des cybercriminels alors que d'autres les voient comme des lanceurs d'alerte. En 2016, ces-derniers avaient infiltré un sous-domaine du ministère de la Défense pour y publier des "leaks" (ou fuite d'informations confidentielles). Dans ce cas, la liberté d'expression et la cybercriminalité s'entremêlent. La cybercriminalité reste un sujet complexe. C'est pourquoi, cette série d'articles explore les différentes facettes de la cybercriminalité.

Article rédigé par le Centre d'information Europe Direct de la Maison de l'Europe de Paris et publié par France-Soir le 28/03/2018