La criminalité électronique et son impact sur la sécurité nationale et la sécurité du citoyen

Docteur Sam Lyes
Professeur en droit, Université de Tizi-Ouzou.

Résumé

La cybercriminalité se définit comme toute activité criminelle réalisée au travers du cyberspace et par le réseau Internet. Par extension, elle intègre toute forme de malveillance électronique effectuée à l'aide des technologies informatique de télécommunication.

De ce fait, la cybercriminalité est une infraction transfrontalière exigeant des Etats une étroite coopération judiciare, technique et opérationnelle dans la prévention et la répression.

Mots clés: cybercriminalité, cyberspace, infraction transfrontalière, coopération judiciare, technologies de l'information.

الملخص

تعرف الجريمة السيبرانية على أنها كل نشاط إجرامي يرتكب من خلال الفضاء السيبراني وعبر الأنترنت. بصورة موسعة، هذه الجريمة تشمل كل شكل من أشكال الأعمال الكيدية الإلكترونية، التي يتم بإستخدام تكنولوجيات الحاسوب والإتصالات السلكية واللاسلكية.

ونتيجة لذلك، تعتبر الجرائم السيبرانية عابرة للحدود وتتطلب من الدول تعاونا قضائيا وتقنيا وعلميا وثيقا في مجال الوقاية والقمع.

الكلمات المفتاحية: الجريمة السيبرانية، الفضاء السيبراني، التهديدات العابرة للحدود، التعاون القانوني، تكنولوجيا المعلوماتية.

Introduction

Chaque technologie est porteuse de potentialités criminelles et offre des possibilités de détournements et d'usage abusif. De tels risques sont inhérents à toutes avancées scientifiques ou technologiques. Alors que l'Internet connaissait une grande expansion, le crime en ligne augmentait également. Les cybercriminels ont largement envahi le monde virtuel, commettant des infractions, tels qu'utilisation de codes d'accès confidentiels, piratage, fraude, espionnage, sabotage informatique, transferts illégaux de fonds et évasion fiscale, trafic de drogue, traite de personne, terrorisme, etc.

Assez souvent, certaines de ces infractions citées à titre non exhaustif, requièrent la participation de plusieurs personnes de différentes nationalités ou résidents dans différents pays. La cybercriminalité est de ce fait une infraction transfrontalière exigeant des Etats une étroite coopération judiciaire, technique et surtout opérationnelle dans la prévention et la répression des infractions électroniques. Les législations nationales devront également s'adapter à l'usage criminel des technologies émergentes.

Aujourd'hui, il existe un risque réel que, sans harmonisation dans ce domaine, les pays qui ont de faibles niveaux de cybersécurité, une législation faible en matière de cybercriminalité et des capacités réduites dans le domaine de l'application de la loi deviennent des refuges pour les cybercriminels.

I. Définition de la Cybercriminalité

La cybercriminalité désigne «toutes les infractions pénales susceptibles de se commettre sur ou au moyen d'un système informatique généralement connecté à un réseau internet. Selon l'Organisation de Coopération et de Développement Economique, la cybercriminalité s'assimile à «tout comportement illégal, ou contraire à l'éthique, ou non autorisé, qui concerne un traitement automatique de données et, ou de transmission de données». De manière générale, il est possible de dresser une typologie des crimes électroniques plus au moins proche de la réalité de la cybercriminalité.

D'une part, il y'a les infractions propres aux technologies de l'information et de la communication, telles que les atteintes aux systèmes de traitement automatisé de données, les traitements non autorisés de don-

nées personnelles, etc. D'autre part, il y'a les infractions commises via les supports de technologies de l'information et de la communication, telles que les infractions financières et économiques, l'enrôlement des terroristes et toute publication à caractère haineux, diffamatoire, etc. Le point commun de toutes ces infractions est qu'elles peuvent être commises à grande échelle. La distance géographique entre le lieu où l'acte délictueux est commis, et ses effets peut être considérable.

Si l'on se réfère à la Convention du Conseil de l'Europe du 23 novembre 2001 (Convention de Budapest)[1], instrument international traitant spécifiquement de la cybercriminalité, on relève neuf types d'infractions. Il s'agit de l'accès illégal aux systèmes et données informatiques, tel que le piratage ; l'interception illégale ; l'atteinte à l'intégrité des données ; l'atteinte à l'intégrité des systèmes ; le marché noir de la production ou la vente de moyens de commettre les infractions ; la fraude informatique ; la falsification informatique ; les atteintes contre des enfants ; les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes.

II. Cybercriminalité et coopération internationale

La coopération internationale en matière de cybercriminalité revêt une importance cruciale parce que la lutte contre ce type de délinquance internationalisée répond à un besoin commun des Etats. La coopération internationale est essentielle pour mener des enquêtes efficaces et traduire les cybercriminels en justice. Toutefois, il est indispensable de substituer aux pratiques traditionnelles de justice pénale des pratiques d'arrestation, de poursuites et de condamnation plus intelligentes. Des mesures de prévention efficaces sont, et continueront à être possibles. Des organisations internationales comme Europol, Interpol et les Nations unies, sont des multiplicateurs de force dans la fourniture d'initiatives multisectorielles efficaces visant à démanteler les réseaux d'ordinateurs zombies, réduire les profits générés par l'économie numérique clandestine et faire activement participer les citoyens à la protection contre les attaques.

La lutte contre la cybercriminalité requiert également la création de centres de spécialistes de l'information et de la coordination du renseignement. Très souvent, ce n'est qu'au niveau international que les analystes

peuvent avoir une idée précise de la portée des activités des groupes cybercriminels et du tort qu'elles causent. Les autorités chargées de l'application de la loi et de la sécurité, par exemple, ont besoin d'organisations comme Europol, Interpol, l'Institut interrégional de recherche des Nations unies sur la criminalité et la justice pour les aider à évaluer la menace et établir des liens cruciaux entre les délits dans des parties du monde souvent très diverses.

III. Cybercriminalité et droit pénal

Sur le plan pénal, « nul n'est responsable que de son propre fait ». La commission d'actes de cyber-délinquance conduit alors à la responsabilité pénale de son propre fait, qu'il s'agisse de l'auteur de l'infraction ou du complice de celle-ci. Toutefois, les actes infractionnels commis sur le web recouvrent des spécificités : qu'en est-il des prestataires techniques et prestataires de services, tels que les fournisseurs d'accès à Internet, les hébergeurs?

Le principe de responsabilité personnelle, conduit à se demander quelle responsabilité pénale peut être encourue par les fournisseurs d'accès à Internet, des hébergeurs et des éditeurs, les hébergeurs sont des personnes physiques ou morales qui assurent des services de communication en ligne permettant le stockage d'écrits, d'images, de sons, de signaux ou de messages de toute nature.

La localisation des infractions recouvre une importance capitale quant à l'applicabilité de la norme sur le plan territorial et à l'identification des cyber-délinquants. Néanmoins, traiter de la localisation des cyber-infractions revient à concilier le caractère délimité de la règle pénale au niveau de l'espace et le caractère universel des réseaux numériques. Ces derniers offrent l'ubiquité et l'immédiateté des échanges d'informations.

En dépit d'une coopération interétatique, la cybercriminalité est régie par les droits pénaux nationaux. Si les conventions internationales permettent de s'acheminer vers l'harmonisation des législations, les souverainetés nationales coexistent, de même que leurs expressions sous forme de réserves étatiques. Ainsi, le droit répressif demeure une expression territo-

rialisée de la souveraineté des Etats. Dès lors, se pose la question de savoir si le critère de la territorialité répond efficacement aux enjeux de la lutte contre la cybercriminalité.

IV. Cadre normatif national de lutte contre la cybercriminalité

La cybercriminalité est avant tout un mode opérationnel, c'est-à-dire la commission d'une infraction par l'un des moyens offerts par les nouvelles technologies de l'information et de la communication.

Ainsi, le législateur algérien s'est inscrit très vite dans la dynamique d'adaptation législative aux nouveaux défis de la criminalité-informatique et ce, à travers les différentes révisions normatives auxquelles il a procédées. Nous les exposerons comme suit :

1- Loi n° 09-04 du 5 août 2009 portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication.

Conformément à l'article 2, on entend par « infractions liées aux technologies de l'information et de la communication » : les infractions portant atteinte aux systèmes de traitement automatisé de données telles que définies par le code pénal ainsi que toute autre infraction commise ou dont la commission est facilitée par un système informatique ou un système de communication électronique.

La présente loi-cadre, régie en des termes techniques les conditions et modalités de la mise en place de dispositifs techniques pour effectuer des opérations de surveillance des communications électroniques, de collecte et d'enregistrement en temps réel de leur contenu ainsi qu'à des perquisitions et des saisies dans un système informatique.

2- Ordonnance n° 66-156 du 8 juin 1966 portant code pénal, modifiée et complétée :

Le droit pénal algérien a connu plusieurs modifications dans le but est de lutter efficacement contre le phénomène de la cybercriminalité.

Ci-dessous, les principaux textes faisant références aux moyens et supports de la technologie et de la communication dans la commission de certaines infractions.

2-1 Loi n° 20-06 du 28 avril 2020 modifiant et complétant l'ordonnance n° 66-156 du 8 juin 1966 portant code pénal :

Art. 196 bis : Est puni d'un emprisonnement d'un (1) an à trois (3) ans et d'une amende de 100.000 DA à 300.000 DA, quiconque volontairement diffuse ou propage, par tout moyen, dans le public des informations ou nouvelles, fausses ou calomnieuses, susceptibles de porter atteinte à la sécurité ou à l'ordre publics.

Art. 253 bis 6 : Est passible de l'emprisonnement d'un (1) an à trois (3) ans et d'une amende de 100.000 DA à 300.000 DA, quiconque diffuse ou divulgue, avant ou pendant les examens ou les concours, les questions et/ou corrigés des sujets d'examens finaux d'enseignements primaire, moyen ou secondaire ou des concours de l'enseignement supérieur ou de la formation et de l'enseignement professionnels ainsi que des concours professionnels nationaux…

Art. 253 bis 7 : La peine est l'emprisonnement de cinq (5) ans à dix (10) ans et l'amende de 500.000 DA à 1.000.000 DA, si les actes mentionnés à l'article 253 bis 6 sont commis par :

- l'utilisation d'un système de traitement automatisé des données ;
- l'utilisation des moyens de communication à distance.

2-2 Loi n° 20-05 du 28 avril 2020 relative à la prévention et à la lutte contre la discrimination et le discours de haine (Abrogeant les articles 295 bis 1, 295 bis 2 et 295 bis 3 de l'ordonnance n° 66-156 du 8 juin 1966, modifiée et complétée, portant code pénal).

Suivant l'article 2 de la présente loi, on entend par Formes d'expression : « Paroles, écrits, dessins, signes, photographies, chants, comédies ou toute autre forme d'expression, quel que soit le support utilisé ».

Aussi, l'utilisation des supports informatiques en vue de propager le discours de haine et de discrimination est une circonstance aggravante de la peine encourue. Ainsi, suivant l'article 31 in fine : « La discrimination et le discours de haine sont passibles d'une peine d'emprisonnement de deux (2) ans à cinq (5) ans et d'une amende de 200.000 DA à 500.000 DA, si : l'infraction est commise par l'utilisation des technologies de l'information et de la communication ».

3- Loi n° 15-12 du 15 juillet 2015 relative à la protection de l'enfant.

Art. 140. Est puni d'un emprisonnement d'un (1) an à trois (3) ans et d'une amende de 150.000 DA à 300.000 DA, quiconque porte ou tente de porter atteinte, par tous moyens, à la vie privée de l'enfant, en publiant ou en diffusant des textes et/ou photographies, pouvant nuire à ce dernier.

Art. 141. Sans préjudice des peines plus graves, est puni d'un emprisonnement d'un (1) an à trois (3) ans et d'une amende de 150.000 DA à 300.000 DA, quiconque exploite un enfant à travers tout moyen de communication sous toute forme et à des fins contraires aux bonnes mœurs et à l'ordre public.

Conclusion

Ces dernières années, l'Algérie connait des mutations économiques et socio-politiques décisifs auxquelles s'ajoutent un contexte régional de plus en plus tendu et menaçant. La cybercriminalité est devenue alors un des moyens les plus redoutables de menace contre la sécurité et la défense nationales. Les adaptations législatives opérées devraient permettre de préserver la sécurité nationale tout en garantissant les libertés fondamentales d'expression et de communication. On le sait, dans certains pays le débat juridique autour de l'incrimination de certaines activités informatiques, porte sur les libertés individuelles en mettant en avant par exemple les principes de nécessité, de proportionnalité et du caractère manifeste d'illégalité. C'est le cas du Conseil constitutionnel français dans sa Décision n° 2020-801 DC du 18 juin 2020 relative à la Loi visant à lutter contre les contenus haineux sur internet.

De ce point de vue, comme le remarque le Professeur David CHILSTEIN, un contrôle accru du respect du principe de nécessité des mesures adoptées apparaît souhaitable, ainsi qu'un rééquilibrage des perspectives d'analyse intégrant davantage la préservation des garanties individuelles et prenant à l'inverse davantage de recul par rapport aux exigences d'une logique strictement policière.

Cette brève réflexion nous a permis de dresser un état des lieux global de la question de la cybercriminalité en droit algérien. Conscient de l'ampleur et de la rapidité des défis posés par la criminalité électronique, le législateur algérien a procédé à la modernisation de sa législation. D'une part, pour une prise en charge pénale du mode opérationnel des cybercriminels. D'autre part, pour protéger les utilisateurs de ces moyens de communication indispensables. La question a pris un caractère multidimensionnel englobant la sécurité des citoyens comme élément indissociable de la sécurité nationale ■

Référence

1. La convention relative à la lutte contre la cybercriminalité s'étend au-delà des seuls Etats membres du Conseil de l'Europe. 55 pays l'ont adoptée dont le Canada (2015), l'Australie (2013), les États-Unis (2007) et le Japon (2012).

Bibliographies

- Brigitte Pereira, La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité, Revue internationale de droit économique 2016/3.
- Myriam Quéméner & Jean-Paul Pinte, Cybersécurité des acteurs économiques : Risques, réponses stratégiques et juridiques, Hermes Science Publications, coll. « Cyberconflits et cybercriminalité », 13 décembre 2012.
- Éric Freyssinet, La cybercriminalité en mouvement, Cachan, Hermes Science Publications, coll. « Management et informatique », 27 septembre 2012.
- Mohamed Chawki, Le droit pénal à l'épreuve de la cybercriminalité, Thèse, Université Lyon III, France, 2006.
- Abbas JABER, Les infractions commises sur Internet, Thèse, Université de Bourgogne, France, 2007.
- Solange Ghrenaouti, La Cybercriminalité les nouvelles armes de pouvoir. 2ème édition, Presse Polytechnique et universitaire romandes, 2018.
- Chilstein David. Législation sur la cybercriminalité en France, Revue internationale de droit comparé. Vol. 62 N°2, 2010.
- Loi n° 15-12 du 15 juillet 2015 relative à la protection de l'enfant.
- Loi n° 20-05 du 28 avril 2020 relative à la prévention et à la lutte contre la discrimination et le discours de haine.
- Ordonnance n° 66-156 du 8 juin 1966 portant code pénal, modifiée et complétée.
- Loi n° 09-04 du 5 août 2009 portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication.