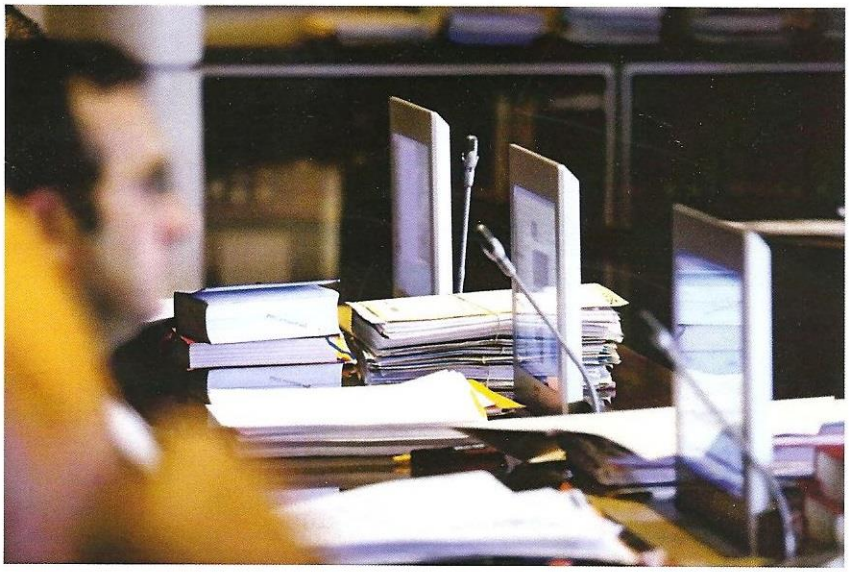
COLLOQUE À LA COUR DE CASSATION

Le droit pénal international face à la cyber criminalité



jeudi 28 juin 2018

de 10h00 à 18h00

en chambre criminelle

5 quai de l'Horloge - Paris 1er

FONDATION SAINT-CYR

COUR DE CASSATION

Le colloque sur le droit pénal international face à la cybercriminalité s'est déroulé le 28 juin 2018 à la Cour de cassation. Organisée par la Chaire Cyber Défense, cette manifestation s'est déroulée à huis clos en présence d'environ quarante représentants des ministères de la Défense, de l'Intérieur, de la Justice et de membres de la société civile. La liberté de parole qui a découlé de cette organisation a pour corollaire la confidentialité des propos qui y ont été tenus. Cette synthèse est établie à l'usage personnel des destinataires et de leurs équipes. Elle n'a pas vocation à être diffusée.

Résumé :

1) Les juridictions doivent faire face, avec la cybercriminalité, à une menace toujours plus importante. Cette mutation a donné lieu, notamment, à la création d'une section cybercriminalité au sein du parquet de Paris.

2) La loi du 3 juin 2016 a doté le parquet de Paris d'une compétente concurrente nationale.

3) La cybercriminalité, par nature volatile et immatérielle, défie les frontières et pose des difficultés tant dans l'application de la loi pénale dans l'espace que pour identifier les auteurs d'infraction.

4) Sur le plan européen, la coopération passe par différents outils. Les plus performants sont l'European cybercrime center (EC3), plateforme d'échange de données opérationnelles, ainsi que les équipes communes d'enquête.

5) Sur le plan international, le texte de référence en matière de cybercriminalité est la Convention de Budapest.

6) La dimension internationale de la cybercriminalité implique d'harmoniser les législations nationales, l'accès à la preuve numérique serait facilité. Pour autant, il ne faut pas oublier la souveraineté des Etats.

SYNTHESE DU COLLOQUE DU 28 JUIN 2018

« Le droit pénal international face à la cyber criminalité »

Allocution d'ouverture : **M. Christophe SOULARD**, président de la chambre criminelle de la Cour de cassation

Propos introductif :

- Ambassadeur Jean-Paul LABORDE, titulaire de la chaire cyber défense, cyber sécurité

- M. Marc PERRIN de BRICHAMBAUT, second vice-président de la Cour pénale internationale

Table ronde n°1 : **Les infractions, l'indentification des auteurs et les enquêtes**

Qualification juridique des faits, qualification pénale des infractions :

Me Cécile DOUTRIAUX, avocat

L'identification de l'auteur de l'infraction :

Colonel Cyril PIAT, représentant du Service central de renseignement criminel

Les investigations, la collecte de preuve :

Chef d'escadron Laurence LALOUBERE, représentante de l'Institut de recherche criminelle, division criminalistique ingénierie et numérique

Colonel Jean-Dominique NOLLET, European cybercrime center, EUROPOL

Table ronde n°2 : **La compétence juridictionnelle**

Débats animés par **Gilles GUIHEUX**, *directeur du centre de recherche des écoles de Saint-Cyr Coëtquidan*

Mme Claudia GHICA-LEMARCHAND, professeur de droit privé et de sciences criminelles à l'université Paris-Est-Créteil

Mme Alice CHERIF, vice-procureur du tribunal de grande instance de Paris, service cybercriminalité, JIRS – compétence nationale, Parquet de Paris

Général d'armée (2S) Marc WATIN AUGOUARD, directeur du centre de recherche de l'école des officiers de la gendarmerie nationale

Table ronde n°3 : **La coopération internationale en matière pénale**

Débats animés par **Jean-Paul LABORDE,** *titulaire de la chaire cyber défense, cyber sécurité*

M. Alexander SEGER, responsable de la division cybercriminalité du Conseil de l'Europe

Ambassadeur Eric DANON

Me Myriam QUEMENER, avocat général près la Cour de Paris

Conclusion : **Ambassadeur Sergio PIAZZI**, secrétaire général de l'Assemblée parlementaire de la Méditerranée et haut fonctionnaire de l'Organisation des Nations Unies

SYNTHESE DES DEBATS :

Allocution d'ouverture : **M. Christophe SOULARD**, président de la chambre criminelle de la Cour de cassation

Le sujet est important par les difficultés qu'il soulève, difficultés rencontrées par ceux qui luttent contre la cybercriminalité. Mais c'est une question qui reste, dans la jurisprudence de la Chambre criminelle, relativement marginale. Il y a ainsi une illustration du décalage temporel entre le moment où un phénomène social naît et celui où il arrive devant la Cour de cassation. Cette dernière n'est pas, pour autant, prise au dépourvue. Les thèmes abordés aujourd'hui sont traités devant la Chambre criminelle, qui est sensible à l'efficacité de la lutte contre la délinquance et consciente de son rôle de protecteur des droits fondamentaux.

Propos introductif : **Ambassadeur Jean-Paul LABORDE**, titulaire de la chaire cyber défense, cyber sécurité

Dans son rapport du 24 juin 2013[1], le Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale, estimait « *essentiel d'appliquer les normes qui découlent du droit international en vigueur régissant l'utilisation de la téléinformatique… afin de réduire les risques pour la paix, la sécurité et la stabilité internationales* ». Le Groupe d'experts ajoutait également que « *Les utilisations malveillantes pouvant facilement être maquillées, il est souvent difficile d'en déterminer les auteurs, lesquels peuvent agir en toute impunité, créant ainsi un environnement propice à une exploitation de plus en plus sophistiquée de ces technologies* ». Il ajoutait également dans ses paragraphes 19, 20 et 21 que « *Le droit international et, en particulier, la Charte des Nations unies sont applicables et essentiels au maintien de la paix et de la stabilité ainsi qu'à la promotion d'un environnement informatique ouvert, sûr, pacifique et accessible. La politique des Etats en matière informatique et leur compétence territoriale pour ce qui est des infrastructures informatiques présentes sur leur territoire relèvent de la souveraineté des Etats et des normes et principes internationaux qui en découlent. Les actions entreprises par les Etats pour assurer la sécurité informatique doivent se faire dans le respect des droits de l'homme et des libertés fondamentales énoncés dans la Déclaration universelle des droits de l'homme et dans les autres instruments internationaux.* »

Les éléments de ce rapport montent les problèmes auxquels nous devons faire face : impunité, responsabilité des personnes, des organisations criminelles et des États, respect des libertés fondamentales et compétence étatique. Il est essentiel de sensibiliser les juristes au plus haut niveau et d'envoyer un signal fort aux criminels qui utilisent la cybercriminalité en leur démontrant ainsi notre volonté de leur faire face.

Les menaces auxquelles nous devons faire face sont multiples, variables et adaptables. Elles portent également des coups très ravageurs à nos économies, à nos services publics, notre défense et notre sécurité. Or, malgré l'obsession justifiée d'attaques étatiques, il ne faut pas négliger les actions de la criminalité transnationale organisée qui pratiquent ces attaques dans

[1] Ref ONU : A/68/98 document diffuse le 30 juillet 2013

le but principalement de chantages, au sens pénal du terme, ou de fraudes. Il faut souligner que 9 sur 10 des attaques cyber proviennent de cybercriminel et induisent *« plus de bénéfices pour les cybercriminels que le trafic de drogues et l'exploitation des êtres humains à des fins sexuelles ensemble.* L'an dernier au mois de mai, une gigantesque attaque informatique a été déclenchée dans plusieurs pays y compris contre le système de santé britannique. Pour résumer l'ampleur de l'attaque, « *Nous avons relevé plus de 75 000 attaques dans 99 pays »*, a noté Jakub Kroustek, de la firme de sécurité informatique Avast. Forcepoint Security Labs, autre entreprise de sécurité informatique, évoque de son côté *« une campagne majeure de diffusion d'emails infectés »*, avec quelque 5 millions d'emails envoyés chaque heure répandant un logiciel malveillant…résultat 16 hôpitaux britanniques bloqués et des entreprises comme Renault affectées.

Face à cette menace, il faut souligner que le maquis juridique est confus. On peut relever plus de 470 infractions se rapportant à la répression de la cybercriminalité. Cela pose des questions de conflits de compétences juridictionnelle. Comment déterminer où l'infraction a été commise ? Comment utiliser la coopération internationale en matière pénale ? Il faut que ces criminels ne restent pas impunis. Sur ces deux derniers points, la Convention de Budapest dont le suivi et la mise en œuvre est assurée par le mécanisme Octopus, apporte des solutions en mettant en place des incriminations cohérentes dans tous les pays qui sont parties à la Convention.

Un dernier point concernant la collecte des preuves sur les logiciels, les portables ou tout autre objet connecté. Une fois que nous aurons insisté sur l'importance de la protection des données personnelles, comment collecter les preuves sur les systèmes informatiques sur le champ de bataille et les transformer en preuves judiciaires ? Un groupe de travail de l'ONU travaille sur ce sujet. Mais il s'agit aussi de la collecte des preuves sur les systèmes informatiques pour rapporter aux autorités judiciaires les éléments dont elles ont besoin afin d'aboutir à la condamnation des auteurs d'infractions de cybercriminalité. A cet égard, la participation du secteur privé dans la collecte des preuves sur les systèmes informatiques et logiciels est déterminante, ce qui bouleverse d'ailleurs nos concepts de séparation entre le public et le privé.

M. Marc PERRIN de BRICHAMBAUT, second vice-président de la Cour pénale internationale

Depuis une trentaine d'années, on voit apparaitre la diffusion de nouveaux instruments numériques. Le domaine cybernétique est celui qui offre les possibilités les plus vastes, aussi bien aux criminels qu'aux enquêteurs, aux procureurs et aux juges. Ces derniers sont exposés à des défis permanents et le champ est en mouvement constant.

Première remarque : le droit pénal international ne comporte pas de règle de procédure uniforme en matière de recueil et d'acceptation de la preuve, de façon générale et à plus dans le domaine des preuves digitales. La pratique est donc très souple et s'en remet aux juges pour décider au cas par cas de la prise en compte de tel ou tel élément de preuve issue du domaine digital. Ainsi, les juges préfèrent statuer sur la recevabilité de la preuve dans le corps de leurs jugements définitifs.

Le poids qui est accordé à ces nouveaux éléments de preuves dans la délibération des juges internationaux dépend de leur opinion quant à l'authenticité desdits éléments de preuves. Les éléments de preuves du domaine digital doivent être présentés par des experts et corroborés par des témoins présents à l'audience.

Deuxième remarque : les tribunaux internationaux dans leur ensemble, considèrent ces éléments de preuves issus du domaine digital comme des pièces documentaires ou comme des documents d'experts et les admettent sous des formes très différentes. Désormais, les recours sont très fréquents par tous les tribunaux pénaux internationaux au registre de communication téléphonique fournis par les opérateurs, au registre de transfert électronique de fonds par une ou plusieurs agences internationales spécialisées et à l'utilisation des médias sociaux et des sources ouvertes qui fournissent beaucoup d'informations, des enregistrements vidéos…Face à cela, il faut que la défense soit associée aux actes d'expertises en amont pour garantir l'équité de la procédure.

Troisième remarque : il y a une nécessité d'authentifier les éléments de preuves digitaux pour permettre leur prise en compte. Ensuite, il faut noter l'acceptation d'éléments de preuves digitaux de la part d'un tiers rendu encore une fois possible par un expert qui en présente son bien-fondé. Il faut, par ailleurs, vérifier la provenance de chacun des éléments de preuve digitaux. Il s'agit de montrer que la chaine de transmission n'a pas été manipulée. Enfin, il faut garantir la pertinence et la validité de ces éléments dans la durée.

Quatrième remarque : la masse de métadata disponible est en croissance exponentielle. A titre d'exemple, sur le continent africain qui est très pauvre, le taux de pénétration des téléphones portables est désormais de 80 % de la population, utilisé pour des activités criminelles. On peut alors se demander comment les acteurs de la justice peuvent avoir des capacités équivalentes à celles des criminels ? Au sein de la Cour pénale internationale, le bureau du procureur s'est doté d'une petite équipe qui utilise la coopération avec d'autres organes au sein de réseaux, ce qui suppose une confiance et une communication importante.

Table ronde n°1 : **Les infractions, l'indentification des auteurs et les enquêtes**

Qualification juridique des faits, qualification pénale des infractions :

Me Cécile DOUTRIAUX, avocat

Cette forme de criminalité est particulière car elle défie les frontières ce qui pose des difficultés pour identifier l'auteur de l'infraction, collecter les preuves de leurs agissements, obtenir la coopération internationale pour organiser les poursuites et la condamnation des cyberdélinquants.

Un état de la menace numérique a été publié et fait état de 63500 infractions en 2017, soit une hausse de 32 %. Au niveau juridique, il n'y a pas de définition légale de la cybercriminalité. On s'accorde à dire que c'est l'ensemble d'infractions qui sont facilitées ou commises par le biais d'un système informatique connecté à un réseau. Mais cela ne résout pas les problèmes liés à la qualification. Les juristes se sont alors référés aux infractions traditionnellement

réprimées par le code pénal. En cas de diffamation sur les réseaux sociaux, par exemple, on se réfère aux textes réprimant la diffamation et l'injure.

Il n'y a donc pas de difficultés particulières concernant les textes, mais davantage concernant la pratique. Il était question de savoir si ces réseaux sociaux pouvaient donner lieu à des infractions publiques ou non publiques. Il y avait des affrontements entre certaines Cour d'appel sur le fait de savoir si l'injure était ou non publique. La Cour de cassation, chambre civile 1, dans un arrêt du 10 avril 2013 a levé l'ambiguïté en déclarant que *Facebook était un espace public, seulement par destination, à savoir qu'il s'agissait de l'existence d'une communauté d'intérêts caractérisée par des inspirations ou des objectifs partagés formant une entité fermée accessible aux seules personnes agrées dans un nombre très restreint*. Elle a conclu *qu'il s'agissait d'injures non publiques*. Cette position peut surprendre et il faudra juger au cas par cas.

Si certaines infractions ne posent pas de difficultés, ce n'est pas le cas concernant le vol de données. Les juristes se sont référés au vol réprimé par le code pénal mais certaines juridictions ont refusé cette qualification. Il n'y a pas de soustraction frauduleuse puisque les données étaient restées en possession de l'entreprise ; même si elles avaient été copiées par le biais d'une clé USB. Les avocats ont alors utilisé l'abus de confiance, ce qui a permis d'obtenir certaines condamnations. Puis, par une loi du 13 novembre 2014, l'article 323-3 du code pénal, permettant de réprimer l'extraction des données d'un système de traitement automatisé de données, a été complété. Le législateur crée de nouvelles infractions pour réprimer cette criminalité particulière. A titre d'exemple, la loi Godfrain du 5 janvier 1988 réprime les atteintes aux systèmes de traitement automatisé de données.

On a également créé des infractions spécifiques concernant l'usurpation d'identité numérique par la loi LOPPSI 2 de 2011. Ainsi, elle est réprimée lorsqu'elle est effectuée sur un réseau de communication publique en ligne, par un nouvel article 226-4-1.

Une autre création du législateur permet de réprimer le « happy slapping » ainsi que le cyber harcèlement grâce à la loi du 4 août 2014. Plus récemment, la loi pour une République numérique du 7 octobre 2016 réprime le « revenge porn ». Cette pratique qui consiste à diffuser des images sexuelles, prises avec le consentement de la personne, sera réprimée s'il n'y a pas d'accord concernant la diffusion en ligne.

Par une loi du 3 juin 2016, les sites terroristes ont également fait l'objet d'une tentative de répression d'une consultation habituelle des services en ligne qui provoquent directement la commission d'actes terroristes ou en faisant l'apologie. Mais cette disposition a donné lieu à une question prioritaire de constitutionnalité. Le Conseil constitutionnel devait se prononcer sur le fait de savoir si cette incrimination était nécessaire, adaptée, proportionnée à l'objectif poursuivi. Il a censuré cette disposition du législateur. Ce dernier a proposé une nouvelle disposition qui a été censurée une seconde fois.

Outre les textes, il convient de se demander comment effectuer la répression sur le terrain de ces agissements criminels. Au niveau international, 82 pays ont ratifié plusieurs conventions internationales pour permettre la répression.

Deux nouvelles stratégies ont été mises en œuvre : le quantum des peines a été augmenté. Suite à cela, l'impact sur les décisions judiciaires a été intéressant. Mais la volonté du législateur n'a pas été suivi d'effet puisque les peines prononcées sont celles qui étaient prévues dans la loi Godfrain du 5 janvier 1988. Sommes-nous incapables de réprimer ces infractions sur le terrain judiciaire ? Le contentieux est encore émergent et assez marginal. Il y a encore beaucoup de plaintes et certains faits ne font pas l'objet de plainte. L'autre stratégie réside, d'une part, dans la responsabilisation des victimes et d'autre part dans un partage de responsabilité ; entre l'administrateur de Facebook et la personne postant des messages sur les murs par exemple.

L'identification de l'auteur de l'infraction :

Colonel Cyril PIAT, représentant du Service central de renseignement criminel

La problématique de l'identification des auteurs est abordée sous l'angle de la distinction entre l'accès à la preuve et la capacité d'exploitation. Deux axes sont énoncés : établir une typologie de preuve ou d'indices et évoquer les problématiques qui se posent au niveau international.

La première preuve en matière de cybercriminalité est celle forensique, qui peut être qualifiée comme celle visant à extraire du support numérique les données et les rendre intelligible. La deuxième, ce sont les indicateurs que l'on va rémunérer. Ainsi, la cybercriminalité fait appel à des relations totalement virtuelles, pour par exemple se rapprocher de l'auteur de l'infraction. Par ailleurs, il est possible d'avoir recours à la traçabilité financière pour les extorsions. Il faut être capable de tracer des paiements en crypto monnaie. Mais la preuve qui est utilisée le plus souvent est celle par réquisition. On l'évoque car il s'agit de considérer la galaxie d'acteurs privés (fournisseurs d'accès à internet, les opérateurs de téléphonie mobile, des hébergeurs, administrateurs de VPN…) qui agissent sur internet. Ils seront mobilisés par les services d'enquête pour retracer l'activité criminelle. Dans cette situation, certains acteurs, les plus petits, acceptent de coopérer et d'autres, par souci de notoriété, refusent de fournir certaines informations. Une démarche conventionnelle est alors mise en œuvre c'est-à-dire qu'il y a une entente entre les besoins des services enquêteurs et les informations que les acteurs privés acceptent de donner. Néanmoins, il y a un écart notable entre la loi pénale française et la loi pénale américaine, en particulier en matière de diffamation, d'injure et de droits de la presse. Face à cette limite, les opérateurs américains traitent, malgré tout, de façon très réactive les sujets touchant à la sauvegarde de la vie humaine et au terrorisme.

La problématique majeure est l'accès à l'information. Cette préoccupation se retrouve dans des territoires où la situation est beaucoup moins normée. Des Etats, des autorités judiciaires/policières voir des opérateurs privés, qui ne sont pas constants. Une tendance nouvelle, de la part de l'opérateur privé ou de l'autorité judiciaire, consiste à demander de lui communiquer un nombre croissant d'informations sur les dossiers pour lesquels leur coopération est sollicitée. Souvent, l'Etat sollicité mène son enquête en interne dans son pays, sur la base des informations qui lui ont été communiquées, procède aux poursuites dans son

pays et communiquera un compte-rendu des personnes interpellées. Est-ce l'orientation vers laquelle la France doit se résoudre ?

Sur le plan Français, le code des postes et communications électroniques est claire sur les données que doivent conserver les opérateurs de communications électroniques. Les textes en vigueur et en particulier la directive européenne de 1995 prévoyait une traçabilité, tout comme la Convention de Budapest qui impose aux lois nationales de prévoir cette traçabilité des clients. Mais, la Cour de justice de l'Union européenne a estimé, concernant un Etat membre, que la conservation devrait commencer qu'après avoir mis en avant des suspicions. En France, il n'y a pas de discrimination et toutes les données sont conservées pendant un an.

Un autre moyen, assez récent, porte sur le recueil de preuve en ligne. Cela est une nouveauté car c'est une déclinaison tant du Code de procédure pénale que de la Convention de Budapest de 2001. Cette dernière autorise à aller chercher des données stockées à l'étranger à condition de mobiliser l'autorité de protection des données compétente. Le dispositif de perquisition en ligne reste simple car le CPP prévoit qu'en présence du mis en cause ou du mis en examen, depuis le domicile de l'intéressé ou depuis le commissariat ou l'unité de gendarmerie, nous procédions en sa présence au recueil des données accessibles depuis un ordinateur situé au domicile ou au bureau. En pratique, la perquisition reste nécessaire car les données sont majoritairement stockées sur le cloud. Un autre volet de la perquisition en ligne est l'enquête sous pseudonyme c'est-à-dire rentrer en contact avec des personnes pour lesquelles il n'y a pas de traçabilité financière ni de traçabilité de connexion afin d'obtenir d'autres informations ou des éléments matérialisant l'infraction. Les textes sont apparus en 2007 et le législateur a étendu le périmètre en 2010 jusqu'à obtenir un dispositif très large (traite des êtres humaines, pédopornographie, apologie du terrorisme, les trafics de médicaments, les trafics d'espèces protégées et toutes les infractions commises en bande organisée y compris une nouvelle référence aux atteintes au système de traitement automatisé de données de l'Etat lorsqu'elles sont commises en bande organisée). Le projet de loi justice qui sera examiné à l'automne doit faire de ce type d'enquête un dispositif de droit commun.

Les investigations, la collecte de preuve :

Chef d'escadron Laurence LALOUBERE, représentante de l'Institut de recherche criminelle, division criminalistique ingénierie et numérique

La criminalistique est l'étude et la pratique de l'application des sciences pour les desseins de la justice. En d'autres termes, c'est l'étude des traces laissées par une action criminelle ou litigieuse, le but étant de retrouver son auteur et son modus operandi. La criminalistique regroupe beaucoup de domaines : la médecine légale, l'odontologie, la biologie, les empreintes digitales mais également la balistique et depuis une vingtaine d'années, l'informatique.

Depuis une vingtaine d'années, la criminalistique numérique devient incontournable. La preuve numérique est, comme la preuve classique, matérielle ou immatérielle. La preuve matérielle numérique réside dans des supports ayant des capacités de stockage sur lesquels on va extraire de l'information mais également des supports sans capacité de stockage (caméra

espion ou des dispositifs d'engin explosif où sera étudié le contenant). La partie immatérielle concerne les fichiers qu'ils soient multimédias (photos, vidéos, sons), bureautiques et la navigation internet. Les ondes et réseaux constituent aussi la partie immatérielle (flux de communications interceptés, identifier ou localiser une adresse réseau à partir de nom domaine, d'adresse IP ou encore découvrir la topologie d'un réseau).

Les moyens de recueil de la preuve sont multiples : la saisie en perquisition, l'interception de communications avec la coopération de l'opérateur, les réquisitions judiciaires auprès des opérateurs de télécommunications, les constatations judiciaires c'est-à-dire la recherche d'infractions sur internet et les utilisations de techniques en milieu ouvert (recherche Google, consultation de bases de données sur internet et des relevés avec des outils de mesure).

La preuve numérique soulève de nombreux problèmes. Une perquisition doit être menée de façon minutieuse afin de ne pas passer à côté d'éléments tels que des disques durs Wifi sans fil, des consoles de jeux qui peuvent contenir des documents personnels et qui peuvent être partagés par internet ou encore des cartes mémoire. Une autre problématique concerne le stockage distant. Chez un particulier, tout n'est pas forcément stocké sur un ordinateur. C'est le cas avec les webmail ou avec le Cloud. Pour l'entreprise, les objets prélevés ne seront pas les mêmes en fonction de la topographie du réseau. L'ordinateur n'est qu'un terminal de saisie et de consultation et aucune donnée est stockée. Les informations sont alors stockées sur un serveur distant.

Cette cybercriminalité a un aspect très technique. Si les outils informatiques présentent des risques, ils ont de nombreux avantages pour les enquêteurs car ils permettent la localisation, l'identification et montrent les différentes stratégies des criminels.

Colonel Jean-Dominique NOLLET, European cybercrime center, EUROPOL

L'European cybercrime center (EC3) est un outil de coopération internationale policière. Le but est de fournir une plateforme d'échange au profit des Etats membres…35 pays avec lesquels EUROPOL échange de la donnée opérationnelle. C'est le seul endroit où la donnée criminelle peut être stockée et croisée avec un cadre juridique de protection des données très fort, à condition qu'elle soit collectée à des fins d'enquêtes criminelles ou de renseignements criminels. Il s'agit d'avoir accès aux enquêtes en cours et d'aider les enquêteurs avec les outils les plus pertinents possible.

Le deuxième élément que propose l'European cybercrime center est un réseau. La cyber regroupe l'ensemble de ces domaines : judiciaire, militaire, technique ou commercial. La problématique est de trouver des nouvelles coopérations pour faire fonctionner cet écosystème, tout en sécurisant internet. C'est une condition primordiale pour développer nos sociétés. En matière de cybercriminalité, il faut travailler en proactivité ; ainsi la réquisition, l'acquisition à la preuve sont essentielles mais ne vont pas résoudre toutes les affaires. Il faut une proactivité à travers un réseau d'acteurs, policiers ou du renseignement dans les domaines tels que la lutte contre l'abus de l'enfant en ligne. Il y a des pays eu sein de l'Union européenne où la pédopornographie, les Pays-Bas par exemple, n'est pas illégale. Le piratage et la fraude en ligne sont également les domaines sur lesquels l'EC3 travaille en proactivité.

Une des clés des services rendus par l'EC3 est de trouver une juridiction compétente en matière de cyber. Comment les forces de l'ordre s'organisent avec les différentes lois qui existent dans chaque pays pour proposer une réponse coordonnée pénale, judiciaire et policière ?

Un autre point important dans le domaine juridique est le raisonnement par analogie. Le besoin de vulgarisation de ce qui se passe dans le monde cyber ou dans la preuve digitale impose de raisonner par analogie en présentant les éléments de façon simplifiée. Le monde informatique est une technologie pour laquelle il n'y a pas encore des années d'expérience. C'est un domaine très complexe, en constante évolution. Ainsi, la proportionnalité est très importante et le droit pénal français amène les enquêteurs à avoir recours à beaucoup d'expertise. Alors que dans le domaine cyber, la vraie difficulté est de savoir si les données qui seront utilisées au procès pénal requièrent une expertise aussi importante que dans une affaire de meurtre par exemple. Que veut-on faire en matière de recueil de preuve pénale en ayant recours à l'expertise ? Quelle est la proportionnalité à adopter dans ce domaine ?

Au sein de l'Union européenne, la France montre une réelle volonté, notamment à travers le législateur, de suivre l'évolution du monde de la cybercriminalité. Mais il y a un problème de moyen ; il y a des affaires où les enquêteurs se retrouvent bloqués dans l'acquisition des données de communication entre des suspects. La proportionnalité est importante face à des affaires plus graves ; sur ce point, la France est un peu en retard.

Un autre point important concerne la connaissance de la cybercriminalité. Il faut démocratiser la connaissance de la cybercriminalité. En réseau, policiers, gendarmes, militaires, magistrats, avocats, techniciens civils, entreprises, doivent discuter pour ne pas se retrouver dépendant du monde civil qui est le seul à fournir des statistiques.

Il convient de retenir que dans cet écosystème si particulier, qu'est le monde cyber, la nécessité d'échanger l'information et de coopérer est primordiale au niveau international. Face à une évolution constante de ce domaine, des difficultés nouvelles vont apparaitre avec la 5G par exemple. Des solutions européennes sont envisageables et devront être mises en avant puisqu'elles assureront la paix et la sécurité des citoyens.

Table ronde n°2 : **La compétence juridictionnelle**

Débats animés par **Gilles GUIHEUX**, *directeur du centre de recherche des écoles de Saint-Cyr Coëtquidan*

Mme Claudia GHICA-LEMARCHAND, professeur de droit privé et de sciences criminelles à l'université Paris-Est-Créteil

La cybercriminalité est par nature immatérielle, internationale et volatile, même si sa trace est matérialisée dans un endroit déterminé et de manière indélébile. Le fait que l'infraction se place dans l'espace numérique pose la question de l'application de la loi pénale dans l'espace. Pour punir le délinquant, il convient de commencer par déterminer quelle loi est applicable, puisqu'elle détermine la juridiction compétente.

Pour les infractions commises en France, le fondement de la compétence pénale est le principe de territorialité mis en exergue à l'article 113-1 du Code pénal disposant « la loi pénale française s'applique aux infractions commises sur le territoire de la République ». Le principe de territorialité est entendu très largement par le Code pénal que ce soit du point de vue spatial, matériel ou personnel. La localisation de l'infraction sur le territoire français est soumise à des critères matériels larges. Le Code pénal assimile l'infraction commise en France à l'infraction réputée commise en France « dès lors qu'un de ses faits constitutifs a eu lieu en France ».

Pour les infractions commises en dehors du territoire, la loi pénale française se teinte d'extra-territorialité et s'applique à des infractions commises en dehors du territoire de la République. Le Code pénal prévoit plusieurs mécanismes de rattachement de l'infraction à la loi pénale française. La compétence personnelle active (article 113-6) prend en compte la nationalité de l'auteur de l'infraction, puisqu'il a joué un rôle actif dans la commission. La compétence personnelle passive (article 113-7) prend en compte la nationalité française de la victime, passive puisqu'elle a subi l'infraction. Elle a été indirectement complétée par l'article 113-8-1 qui intervient dans le cadre d'une infraction commise à l'étranger par un étranger sur un étranger, ne bénéficiant d'aucun rattachement, ni territorial, ni personnel, à la loi française. Il s'agit en réalité d'une compétence de substitution puisque la France se substitue au pays auquel elle a refusé le droit de faire Justice. Le Code pénal utilise aussi la compétence réelle fondée sur la matière concernée par l'infraction qui porte atteinte aux intérêts essentiels de la France.

Enfin, l'application extraterritoriale de la loi française est renforcée par la compétence universelle reposant cumulativement sur le droit national et le droit international. L'universalisme de l'interdit et la gravité de certains comportements déclenchent l'application de la loi pénale française alors même que l'infraction est commise à l'étranger, par un étranger sur un étranger (article 689-1).

Le droit pénal a dû innover pour suivre l'évolution et le développement numérique de la délinquance. La jurisprudence hésitante et contradictoire entre différentes chambres de la Cour de cassation a conduit le législateur à adapter le Code pénal à la modernité de la cybercriminalité, tout en restant fidèle aux mécanismes classiques de la détermination de la compétence pénale.

La loi du 3 juin 2016 a introduit l'article 113-2-1 dans le Code pénal prenant en compte spécifiquement le moyen de commission de l'infraction. L'infraction numérique est réputée commise en France et déclenche le principe de territorialité. Cependant, l'utilisation d'un réseau de communication électronique n'équivaut pas à « un fait constitutif commis en France », mais fait naître une présomption de rattachement au territoire français. D'une partie de l'infraction commise en France, nous passons à une infraction virtuellement commise en France. Cette présomption a vocation à s'appliquer à toutes infractions commises par le vecteur numérique.

Si le mécanisme semble reposer sur la territorialité, il se fonde aussi sur la compétence personnelle et la compétence réelle. D'une part, l'infraction doit être commise au « moyen d'un réseau de communication électronique ». Il est possible de remarquer que le mode de

commission de l'infraction – le moyen numérique – devient le principal critère de rattachement à la loi pénale française.

D'autre part, la loi pénale française s'applique lorsque l'infraction est commise « au préjudice d'une personne physique résidant sur le territoire de la République ou d'une personne morale dont le siège se situe sur le territoire de la République ». Il apparaît clairement que le mécanisme retenu est la compétence personnelle passive prenant en compte la victime de l'infraction et assimilant les personnes physiques et les personnes morales, mais semble exiger, selon certains auteurs, une identification de la victime. Pour la personne physique, le critère est la résidence sur le territoire de la République. La compétence personnelle passive profite aussi aux personnes morales « dont le siège se situe sur le territoire de la République ». Le législateur reste fidèle au mécanisme classique de nationalité, puisqu'en droit commercial, le siège de la société équivaut à la nationalité de la personne physique.

Enfin, une dernière question se pose car l'infraction doit être commise « au préjudice » de la personne physique ou morale. La jurisprudence de la Chambre criminelle l'interprète très largement et admet qu'il puisse être aussi bien moral que matériel et, plus encore, qu'il soit simplement éventuel et pas nécessairement effectif. Il ne sera pas nécessaire à la victime de démontrer qu'elle a subi un préjudice et de le chiffrer, il lui suffira de démontrer sa potentialité.

Si la compétence légale française en matière de cybercriminalité paraît exceptionnelle, elle mobilise des mécanismes classiques et les exploite dans un contexte d'efficacité et d'évolution technologique constante, ce qui se continue dans la détermination de la compétence juridictionnelle elle-même.

Mme Alice CHERIF, vice-procureur du tribunal de grande instance de Paris, service cybercriminalité, JIRS – compétence nationale, Parquet de Paris

Une fois que la loi française est applicable dans ces phénomènes où la criminalité se manifeste au niveau mondial et dans l'espace numérique, il a été créé au sein du parquet de Paris, la section cybercriminalité. Cette création répond au constat qu'il y a eu une véritable mutation liée à notre monde hyper connecté où les données sont à la fois économiques, stratégiques, vitales et celles-ci sont convoitées. Cette section, dont la création a été décidée en septembre 2014, est dédiée à la cybercriminalité stricte c'est-à-dire quand le système d'information et le moyen de communication ne sont pas tant les vecteurs d'une autre infraction de droit commun mais lorsque ce système et ce moyen de communication sont eux-mêmes objet de l'infraction. Ce sont les articles 323-1 et suivant du CPP qui régissent les dispositions venant caractériser les infractions poursuivies, qui sont l'atteinte au système de traitement automatisé de données. Elles ont été introduites dans le Code pénal par la loi du 5 janvier 1988 dite Godfrain. L'article 113-2-1 du Code pénal a créé une révolution pour le parquet. Avant la loi du 3 juin 2016, lorsqu'une plainte était déposée, se posait d'abord la question de déterminer la compétence du parquet, art. 43 du CPP, mais difficilement applicable en matière de cybercriminalité. De même, pour déterminer le lieu des faits, un arrêt de la Chambre d'instruction de la Cour d'appel de Paris du 3 mai 2008 considérait comme étant le lieu des

faits, le siège de la victime, le siège du maitre du système qui a à subir les effets de l'attaque. Quant au parquet de Nanterre, il retenait comme lieu des faits, celui de domiciliation du serveur. La loi du 3 janvier 2016 a mis fin à ces différences d'interprétation. Le parquet de Paris est dorénavant compétent pour les infractions sur les systèmes de traitement automatisé des données au préjudice de victimes basées à Paris ou établies sur le ressort de la JIRS (Juridiction interrégionale spécialisée). La cybercriminalité ne tenant pas compte des contours des ressorts des tribunaux, ce critère concernant les JIRS a été mis en place afin d'éviter un émiettement des enquêtes.

Avant le 3 juin 2016, seulement douze affaires avaient été retenues au titre de la JIRS. En revanche, le lien de connexité était le moyen procédural le plus pertinent pour permettre au parquet de Paris de reprendre des enquêtes, qui devait néanmoins être en charge d'une enquête première. A partir de cette loi, les dispositions des articles 706-72-1 du CPP ont doté l'ensemble de la juridiction parisienne d'une compétence concurrente nationale en matière d'atteintes au système de traitement automatisé de données. Cette compétence s'étend jusqu'à la Cour d'assises car il a été créé par cette même loi une infraction pénale informatique criminelle, celle de sabotage informatique.

En fonction de l'ampleur des faits, les enquêtes sont confiées à différents services, et notamment à un service spécialisé de la Direction Centrale de la Police Judiciaire, l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication. Ce service intervient notamment lorsqu'il y a un très grand nombre d'auteurs ou de victimes et lorsque l'enquête nécessite une investigation sur l'ensemble du territoire. Des enquêtes sont également confiées au C3N qui relève du pôle judiciaire de la gendarmerie nationale. Et lorsque les faits portent sur des opérateurs d'importance vitale, c'est la Direction générale de la sécurité intérieure qui est saisie. Mais le service qui reste le plus souvent saisi est la BEFTI (Brigade d'enquêtes sur les fraudes aux technologies de l'information).

Il existe des critères d'exercice de cette compétence concurrente nationale. Le premier concerne les faits, lorsqu'ils dénotent d'un haut degré de technicité c'est-à-dire un mode opératoire innovant. Le deuxième concerne la dimension internationale au regard de la configuration des faits par exemple. Par ailleurs, le parquet de Paris est également saisi au regard de la complexité procédurale de l'affaire, soit car il y a un nombre de victimes trop important ou un nombre d'auteurs vaste. Enfin, le parquet de Paris s'occupe des affaires portant sur des cibles sensibles des systèmes gouvernementaux ou institutionnels qui participent au bon fonctionnement de la nation.

Général d'armée (2S) Marc WATIN AUGOUARD, directeur du centre de recherche de l'école des officiers de la gendarmerie nationale

Le droit pénal et la cybercriminalité sont deux domaines totalement opposés. Le droit pénal est un droit régalien. A l'inverse, la cybercriminalité est sans frontière et les effets sont transfrontaliers. Comment faire cohabiter le droit pénal, enfermé dans des frontières, et la cybercriminalité, phénomène planétaire ? L'article 113-2-1 du code pénal issu de la loi du 3

juin 2016 a pour volonté d'élargir la compétence du juge français, au regard notamment du lieu de résidence de la victime.

Une deuxième remarque porte sur l'espace numérique qui est, par construction, international. Malgré une tentative de balkanisation politique avec des pays qui se renferment, on arrive toujours à communiquer et cet espace est poreux. C'est un nouveau phénomène criminel qui émerge avec un démembrement spatio-temporel. Il n'y a plus d'unité de temps, ni de lieu et d'action.

L'apparition de la cybercriminalité dans le droit pénal remonte à 1978. Les premiers articles du code pénal concernent le traitement illégal de données issu des lois informatique et liberté puis Godfrain. Au départ, c'était un contentieux d'exception, qui a considérablement augmenté, et conduit les tribunaux et les services de police à se reformater. Il y a une double transhumance : celle du délinquant qui a compris que le cyberespace apporte un meilleur cout-efficacité. En effet, une escroquerie dans le cyberespace rapporte davantage que dans le monde réel. Par ailleurs, la guerre dans l'espace numérique effectue une transhumance par la cybercriminalité.

Face à une cybercriminalité de plus en plus difficile à maitriser par les voies judiciaires, la tentation est grande de voir un déplacement vers la police administrative, vers la prévention, vers le renseignement … tous ces domaines qui échappent au juge judiciaire. Il est judicieux de se demander si le pouvoir judiciaire n'abandonne-t-il pas, au profit du préventif, le travail qui lui incombe.

Les années à venir vont apporter des changements notables. Jusqu'à maintenant, on partageait du droit souverain tout en les harmonisant entre les différents pays et en créant des traités bilatéraux afin que les droits deviennent compatibles. Aujourd'hui, on essaie de partager des règles de droit aussi communes que possible pour pouvoir avancer dans la coopération entre les pays. Dans ce contexte international, la donnée, qui est la preuve, est au cœur de la transformation numérique et de la problématique de la lutte contre la cybercriminalité. Il y a une véritable guerre de la donnée, avec pour commencement l'affaire Snowden.

A terme, il faudrait arriver à une entente entre les pays qui partagent la même vision du droit. Sans cela, on risque d'aller vers une négation totale de la souveraineté d'autrui, pour avoir un cyberespace conçu dans un désordre public total au sein duquel le juge ne trouvera plus de repère.

Débat suite à la table ronde n°2 :

Face à cette délinquance qui progresse et qui évolue, il faut reformater. C'est une délinquance où le gain est très élevé pour un risque le plus faible ; les peines prononcées aujourd'hui, ne sont pas considérables. Le droit a déjà commencé à s'adapter. La Chambre criminelle a différentes possibilités : elle a utilisé des qualifications traditionnelles, elle a transféré des QPC afin d'obtenir une réaction de la part du Conseil constitutionnel…dans le but d'attirer l'attention du législateur afin de combler certains vides juridiques.

Intervention d'Eric Danon : Il faut différencier deux choses qui ne sont pas de mêmes natures : le cybercrime (malware…) et le crime normal dont la commission a été permise grâce à l'utilisation de moyens numériques. D'un côté, le numérique est au service du crime et de l'autre, le crime rentre dans le monde du numérique. C'est toute l'ambiguïté de l'article 133-2-1. La deuxième difficulté relève de la donnée. Lorsque cette dernière est volée, c'est la différence d'un vol classique, la victime n'est plus la seule à l'avoir. Par ailleurs, à qui appartiennent toutes ces données ? Cela représente une difficulté pour la France lorsqu'elle doit négocier avec d'autres pays.

Table ronde n°3 : **La coopération internationale en matière pénale**

Débats animés par **Jean-Paul LABORDE,** *titulaire de la chaire cyber défense, cyber sécurité*

Il y a une convergence entre la notion de crime qui a une résonnance internationale, ce sont les crimes cyber, et les crimes déjà répertoriés qui ont besoin de la cybercriminalité. Ces derniers nécessitent une coopération internationale. Il faut combiner les deux, au sein de la coopération pénale en matière pénale, à l'aide de différents outils : les enquêtes conjointes et le transfert de procédure. Au-dessus de ces outils, le texte fédérateur est la Convention de Budapest.

M. Alexander SEGER, responsable de la division cybercriminalité du Conseil de l'Europe

La Convention de Budapest couvre les infractions en matière de cybercriminalité et les questions de preuve électronique liées à toute infraction en lien avec un ordinateur.

L'approche du Conseil de l'Europe en matière de cybercriminalité passe par trois éléments. Le premier est le standard commun avec la Convention de Budapest mais aussi la protection des données, le terrorisme, le blanchiment d'argent, la protection des enfants…Puis, il y a le comité sur la cybercriminalité (T-CY) qui effectue des analyses de la mise en œuvre de la Convention. Il peut également négocier des protocoles additionnels. Le troisième élément concerne le renforcement des capacités pour aider les pays à mettre en œuvre les différentes recommandations du comité.

La Convention couvre deux éléments : le droit pénal matériel, c'est-à-dire les atteintes contre et à travers le système informatique. Le deuxième élément est le droit procédural avec les questions de preuve électronique.

Cette convention est complétée par un protocole additionnel sur la xénophobie et le racisme depuis 2003 mais aussi par des notes d'orientation adoptées par les parties à la Convention. Par exemple, des notes d'orientation ont été adoptées pour expliquer quelles sont les articles de la Convention couvrant les phénomènes de « botnets » ou de « Malware ». Une note d'orientation concerne l'article 32 de la Convention sur l'accès transfrontalier et une portant sur l'article 18 couvre les injonctions de produire. Il y a maintenant une possibilité, grâce à cette note d'orientation, de demander aux fournisseurs d'un service des informations sur les abonnés. Il y a également depuis septembre 2017, une négociation pour un protocole additionnel.

La portée géographique de la Convention de Budapest. Il y a 59 pays qui l'ont déjà ratifiée. Sur les 193 pays membres des Nations unies, seulement 95 ont des législations en conformité avec la Convention de Budapest. Les Etats sont de plus en plus nombreux à utiliser cette convention, même s'ils n'y ont pas encore adhéré.

L'enjeu majeur se situe dans la preuve électronique. Où est la preuve ? Qui est responsable ? Lorsque les données sont stockées sur le Cloud, la localisation de ces dernières est difficile à établir. Et la question du régime juridique applicable se pose. Au regard de ces difficultés, il faut tout d'abord établir une distinction concernant le type d'information nécessaire (celle sur les abonnés, sur le trafic et sur le contenu). Chacune de ces informations obéit à des règles spécifiques. Par ailleurs, la question de l'efficacité limitée de l'entraide judiciaire se pose ou encore celui de la localisation des données. Une étude a été effectuée à propos des fournisseurs aux Etats-Unis (Apple, Facebook, google, Microsoft, Twitter et Yahoo). Une demande directe est envoyée afin d'obtenir des informations sur les abonnées et dans 60 % des cas, une réponse est donnée.

Les solutions proposées dans le cadre de la Convention de Budapest sont au nombre de cinq : rendre l'entraide judiciaire plus efficace, note d'orientation sur l'article 18 adoptée en février 2017, des règles internes pour les injonctions à produire (CEDH, Benedik v. Slovénie), mettre en œuvre des mesures pratiques de coopération avec les fournisseurs et négociation d'un protocole additionnel. Ce dernier n'est pas seul. Il y a également des propositions de l'Union européenne sur la preuve électronique ainsi que le Cloud Act. Il est nécessaire de trouver une cohérence.

Il y a deux éléments qui sont compliqués : la coopération directe avec les fournisseurs de services d'autres juridictions et l'accès transfrontalière aux données, dû à la souveraineté des Etats ainsi que la protection des données des individus.

Ambassadeur Eric DANON

Il y a des difficultés conceptuelles. La première, le droit français n'arrive pas à distinguer, le crime cyber (les malwares, le fishing…) c'est-à-dire un crime de nature informatique et les crimes normaux pour lesquels le numérique a servi de façon accessoire ou essentielle. Dans le premier cas, si c'est un crime de nature cyber, la question est celle de l'incrimination. Dans l'autre cas, le problème est la recherche de preuves. Cette distinction n'existe pas dans le droit français. L'article 113-2-1 connaitra des limites lorsqu'il faudra travailler à l'international.

La deuxième, c'est que le crime est presque transnational, non pas par nature mais de fait. Dans les crimes de nature informatique, il est très rare que les attaques dans un pays viennent du même pays. En France, moins de 5 % des crimes viennent de France. Dans le deuxième cas, l'utilisation du numérique pour commettre un crime, le seul fait que la plupart des serveurs informatique ne soient pas en France, entraine une recherche de la preuve à l'international. Ainsi, dans les deux cas, l'action relève très rarement d'un seul pays.

Troisièmement, les lois restent nationales. Dans cette hypothèse, soit une loi commune est créée soit on cherche à coopérer. Les négociations sont complexes car les Etats-Unis est un partenaire qui maitrise très bien le sujet. La majorité des données des français sont stockées aux Etats-Unis et ils ont une compétence de fait, en raison des discussions permanentes avec les fournisseurs de services. Dans la pratique, la situation est favorable aux américains.

Enfin, l'extra-territorialité n'est pas un élément positif pour la France, notamment dans le rapport de force qu'elle introduit avec les Etats-Unis. Mais le problème étant international ou transnational, l'extra-territorialité n'est pas mauvaise par nature. La France a donc besoin du Cloud Act, même s'il permet aux américains de rentrer dans des données personnelles françaises de citoyen français, car il serait utile pour les enquêtes françaises. Ainsi, la question est celle de la réciprocité à travers la volonté de créer un accord d'entraide judiciaire avec les américains. La Commission européenne a voulu créer un texte commun à tous les pays européens, les Etats-Unis ont refusé. Un nouveau texte, e-evidence, présente des éléments allant au-delà du Cloud américain. D'où, la possibilité, s'il entrait en vigueur, pour une entreprise qui se trouverait en difficulté sur le sol européen de fournir des informations au titre du texte e-evidence. Le texte prévoit également une obligation de conserver les données.

La preuve numérique soulève un autre problème ; connaissant la possibilité de transformer les data, quelle est la validité, l'intégrité de cette preuve fournie ? Lorsque Microsoft envoie des données, sa capacité à les modifier est colossale. Enfin, l'admissibilité même de la preuve pose problème. Sans un accord d'entraide judiciaire entre deux pays, est-il possible de s'adresser directement à Apple par exemple ? Quelle est la recevabilité de ces informations dans un procès ?

Pour conclure, il n'y pas encore véritablement de cadre pour l'accès à la preuve numérique. Le problème majeur est la territorialisation d'un système qui, par nature, est déterritorialisé.

Me Myriam QUEMENER, avocat général près la Cour de Paris

Les normes pénales classiques peinent parfois à s'adapter à la cybercriminalité. Les données numériques constituent désormais un réel enjeu de pouvoir entre les États qui veulent s'assurer le contrôle sur celles qui circulent sur leur territoire, et entre les entreprises privées qui fournissent les réseaux qu'elles empruntent.

Les données et leur maîtrise reconfigurent les rapports de force au plan stratégique et économique et donnent lieu à de nouvelles représentations de souveraineté. La dimension internationale de la cybercriminalité implique d'harmoniser les législations nationales ou à tout le moins, de faciliter la coopération sur le plan européen et international.

Lorsque les prestataires ne sont pas établis dans l'Union européenne, il convient d'avoir recours à une demande d'entraide pénale internationale. Les enjeux sont très forts et il ne faut pas négliger leurs aspects géopolitiques et stratégiques avec l'émergence de législation extraterritoriale risquant de porter atteinte à l'Europe comme le Clarifyng Lawful Overseas use of data Act ou Cloud act.

Ainsi, il se superpose un affrontement dans le cyberespace, dans un mélange de défense de la souveraineté nationale et de recherche de l'extraterritorialité la plus large. Il convient de ne pas négliger la menace de la captation des données par un oligopole d'entreprises. Face à ce phénomène, la France construit une législation protectrice d'une part de ses systèmes d'information avec la directive Network information security (NIS) d'autre part de ses données personnelles avec le Règlement Général sur la Protection des Données (RGPD).

Parmi les améliorations et les perspectives, l'Union européenne s'est dotée de dispositifs de coopération policière et judiciaire facilitant la lutte contre l'insécurité. Le plus performant d'entre eux est l'équipe commune d'enquête.

L'Union européenne a en effet très tôt perçu les enjeux entourant la cybercriminalité. C'est donc en ce sens qu'elle a mis en place en janvier 2013 le centre européen de lutte contre la cybercriminalité au sein d'Europol (l'office européen de Police). Ce centre aussi appelé EC3 (pour *European CyberCrime Cente*r) a donc pour objectifs principaux de lutter contre la cybercriminalité.

Au niveau des textes, la convention dite de Budapest du Conseil de l'Europe sur la cybercriminalité signée le 23 novembre 2001 demeure l'instrument international contraignant de référence en matière de lutte contre la cybercriminalité. Un deuxième protocole additionnel à cette convention est en cours de rédaction depuis septembre 2017 qui envisage des mesures visant à simplifier la coopération judiciaire entre les 56 pays adhérents à la convention et à faciliter la coopération directe avec les fournisseurs de services sur Internet des autres pays membres.

Dans le cadre de l'Assemblée générale des Nations Unies, la Commission pour la prévention du Crime et la Justice pénale a été chargée de constituer en 2011 un groupe intergouvernemental d'experts (IEG), dédié à la rédaction d'une étude approfondie sur le phénomène de la cybercriminalité. Il a été mis en évidence une division de la communauté internationale sur l'opportunité de compléter ou non le cadre juridique existant. Une majorité d'États, dont la France se sont prononcés en faveur de l'utilisation de la Convention de Budapest comme base juridique pour la lutte contre la cybercriminalité.

La directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale[2] présente l'intérêt d'unifier le droit européen de la recherche de la preuve. En outre, une nouvelle directive proposera d'élargir le champ des infractions relevant de la cybercriminalité en y incluant les transactions effectuées par le biais des monnaies virtuelles. Elle introduira également des règles communes relatives au niveau des peines. Par ailleurs, elle clarifiera la portée de la compétence juridictionnelle des États membres en ce qui concerne ces infractions et garantira les droits des victimes de la cybercriminalité. Enfin et en renforçant la coopération en matière de justice pénale à l'échelle européenne, la directive aura pour objectif de faciliter l'accès transfrontalier aux preuves électroniques.

La Commission européenne a présenté un projet de directive et un projet de règlement e-evidence sur l'accès aux preuves électroniques en matière pénale. L'objectif est de procurer une sécurité juridique aux entreprises et aux prestataires de services en appliquant des règles identiques pour ordonner la fourniture de preuves électroniques. Ces textes prévoient notamment de créer une injonction européenne de production ou encore d'empêcher l'effacement de données au moyen d'une injonction européenne de conservation. Les nouvelles règles imposent également de désigner un représentant légal dans l'Union afin que tous les prestataires soient soumis à des obligations identiques.

Au-delà des textes, la coopération entre les forces de l'ordre et le secteur privé apparait comme la pierre angulaire des affaires à dimension internationale. En outre, n'oublions pas qu'en 2020, le parquet européen sera une réalité, ouvrant ainsi la voie d'une coopération renforcée, 20 États (bientôt 21 avec les Pays-Bas) se sont engagés à concéder une partie de leur souveraineté afin de lutter plus efficacement contre les atteintes aux intérêts financiers de l'Union européenne.

Pour conclure, il apparait indispensable et nécessaire que l'Europe s'inscrive dans une stratégie de gouvernance afin de défendre tant les entreprises que les citoyens face au fléau que représente désormais la cybercriminalité.

Conclusion : **Ambassadeur Sergio PIAZZI**, secrétaire général de l'Assemblée parlementaire de la Méditerranée et haut fonctionnaire de l'Organisation des Nations Unies

Les besoins en opérabilité sont les mêmes, non seulement au sein de l'Union européenne mais également avec d'autres pays, tels que le Maroc, la Tunisie, l'Egypte, l'Algérie, au Liban … Le secrétaire général de l'ONU estime que « la ligne contre le terrorisme est le cyberespace. Les terroristes utilisent les médias, les communications cryptées et le dark web effectuer sa propagande, faire du prosélytisme et coordonner les attaques ». Il existe un lien entre le terrorisme et la criminalité organisée dans le trafics d'armes, dans le trafic d'êtres humains et dans le financement des mouvements terroristes.

Il y a beaucoup d'activités menées au niveau de l'Europe, du Conseil de l'Europe, de l'OTAN et au niveau parlementaire, un soutien essaie d'être donné au niveau national. L'Assemblée parlementaire de la Méditerranée a établi un lien très étroit avec la commission contre le terrorisme du conseil de sécurité de l'ONU et a reçu la mission d'évaluer de façon systématique, par exemple, les résolutions contre Daesch ou celles portant sur la déradicalisation.

La recherche de l'amélioration de l'opérabilité entre les pays est toujours présente ; elle passe par la création d'un glossaire qui serait commun à tous les pays ou encore une liste de solutions possibles à mettre en application face à une éventuelle expulsion par exemple.

La coopération internationale est primordiale. Pour autant, elle nécessite un cadre précis afin de ne pas multiplier les initiatives qui nécessitent beaucoup de ressources sans obtenir les résultats attendus.