Cybercriminalité : Une réalité protéiforme mal définie

par **Faten SKAF***

Résumé
Depuis que les technologies de l'information existent, les réponses juridiques à leur utilisation abusive font légion. En effet, l'évolution de ces technologies demande sans cesse de nouvelles solutions juridiques. Cependant, à cause de leur incontrôlable mutation et de la spécialisation nécessaire à la compréhension de ces technologies, le droit a souvent été rapidement dépassé. Définir la cybercriminalité est extrêmement délicat, tant le phénomène se développe et apporte toujours davantage de faits qualifiés ensuite d'infraction par le droit. En outre, l'étendue de la cybercriminalité mène le droit à être applicable dans plusieurs domaines. Ainsi, le respect de la vie privée, de la vie professionnelle, du droit d'auteur, la liberté d'expression, la protection des biens immatériels des entreprises, etc. sont autant de domaines applicables à la cybercriminalité.

Mots-clés : concept, définition, droit pénal, cybercriminalité, criminalité informatique, cyberespace, Internet.

Summary
Since information technologies have existed, there have been many legal responses to their misuse. Indeed, the evolution of these technologies constantly requires new legal solutions. However, because of their uncontrollable change and the specialization needed to understand these technologies, the law has often been quickly overtaken. Defining cybercrime is extremely delicate, as the phenomenon develops and brings more and more facts that are then qualified as offences by law. In addition, the scope of cybercrime leads the law to be applicable in several areas. Thus, respect for private life, professional life, copyright, freedom of expression, protection of intangible assets of companies, etc. are all areas applicable to cybercrime.

Keywords : Concept, definition, criminal law, cybercrime, computer crime, cyberspace, Internet**.**

Introduction

Comment définir la cybercriminalité ? Comment la prévenir ? Comment la sanctionner ? Comment la réparer ? Répondre à de telles questions suppose d'abord de décrire le phénomène. Dans ce cas, il relève de la responsabilité de l'État de décrire l'étendue comme la complexité de cette délinquance. Or, le concept même de cybercriminalité est équivoque et reste encore pour les professionnels du droit une notion abstraite et incomprise. La cybercriminalité ne renvoie pas à une liste d'infractions bien déterminées, puisqu'elle vise l'ensemble du champ pénal. L'apparition d'un nouveau phénomène entraine nécessairement des difficultés de définition.

* Docteur en droit privé et sciences criminelles, Université d'Aix-Marseille

I. Les problèmes relatifs à la définition de la cybercriminalité

Le droit pénal est désormais face à un nouvel espace qu'il ne peut ignorer, à savoir le cyberespace. C'est dans cet univers que va se développer la cybercriminalité qui concernera progressivement l'ensemble du champ du droit pénal. Le Code pénal a été modifié au coup par coup, au fil des lois comportant des dispositions pénales ayant trait aux technologies de l'information et de la communication et en particulier suite aux attentats terroristes et à l'émergence de nouveaux comportements facilités par le numérique. L'inflation des textes concernant la cybercriminalité, leur complexité, accompagnée de leur superposition ou juxtaposition voire contradiction (1), ainsi que la multiplication des autorités peuvent avoir pour conséquence de rendre délicate l'appréhension juridique des situations rencontrées dans le monde du numérique.

A. Les problèmes non juridiques

La cybercriminalité est l'une des nouvelles formes de criminalité ou de délinquance sur le réseau Internet, dont les conséquences se révèlent être particulièrement graves pour la sécurité. La dangerosité de ce phénomène est due à sa spécialisation, à son caractère mondial d'un coté et d'un autre coté à l'organisation de ses acteurs (2).

1- Les particularités criminologiques de la cybercriminalité

La cybercriminalité présente des particularités criminologiques certaines. En effet, il est devenu classique de la présenter sous les traits d'une délinquance marquée essentiellement par l'immatérialité de son objet (3), l'internationalité de ses implications (4), l'anonymat de ses acteurs (5), l'évolution très rapide des techniques et des stratégies (6) et par la fugacité de ses contenus (7). Ces caractéristiques essentielles sont difficilement cernables par le droit positif français, et par les droits positifs des États.

2- La transnationalité des infractions

Les infractions informatiques ont le plus souvent un caractère international, alors que les informations en elles mêmes sont des données régies par le droit national. En effet, les données des réseaux informatiques internationaux peuvent être transférées à la fois sous une forme cryptée et non cryptée à l'autre bout de la planète en quelques millisecondes sans être soumises à des mécanismes de contrôle efficace par les États. La cybercriminalité a donc un caractère international et pose des défis aux systèmes de justice pénale en place (8). Ces derniers se fondent en effet sur le concept de contrôle territorial et ont du mal à répondre au besoin d'un contrôle sur un cyberespace mondial (9).

3- Le sentiment d'impunité partagé entre les cybercriminels

Les cybercriminels profitent de toutes les facilités offertes par les technologies du numérique et des failles humaines, technologiques, juridiques ou pro-

cédurales, que cela soit sur le plan national ou à l'échelle internationale. Cela est facilité notamment par le fait que :

- Tous les pays ne disposent pas forcément de la même volonté politique de lutter contre la cybercriminalité, ni des structures organisationnelles ou des ressources permettant de le faire ;
- Les procédures liées à l'entraide internationale des forces de justice et de police sont souvent complexes et longues ;
- Les traces numériques peuvent être brouillées, effacées ou fausses. De plus, les traces numériques sont difficiles à collecter et à interpréter. Elles ne permettent pas toujours de remonter jusqu'à l'identité des criminels ;
- Les cybercrimes se réalisent le plus souvent en impliquant de multiples acteurs aux compétences particulières et savoir-faire spécialisés dans des tâches spécifiques, séparées et restreintes. Ces acteurs se regroupent en fonction de projets criminels à durée déterminée. Ils se constituent en équipes virtuelles réparties dans le monde entier, ils travaillent ensemble pour des missions ciblées en recrutant des compétences ou en utilisant les outils nécessaires pour mener à bien une activité criminelle, en prenant le moins de risque possible.

B. Les problèmes juridiques

La cybercriminalité n'échappe pas à la problématique de sa définition, qui tient en particulier à la difficulté de cerner cette forme de criminalité dans l'espace Internet (10). La difficulté de la conceptualisation de la cybercriminalité est liée non seulement au manque de définition légale de cette notion, mais aussi à la manière dont celle-ci se présente sur le plan pratique. Le champ de cette délinquance électronique est plus difficile à appréhender ; il est vaste et hétérogène parce qu'il englobe un grand nombre et une grande variété d'activités de par le monde. De même, les pratiques et les objectifs des acteurs impliqués varient grandement. En outre, une même pratique peut avoir divers objectifs et, inversement, un même objectif peut être réalisé à l'aide de pratiques différentes. Mais quelles sont les difficultés qui contribuent au sentiment de flou que suscite ce concept et donc à son appréhension (11) ?

1- L'absence volontaire de définition juridique

Le terme de cybercriminalité demeure difficile à conceptualiser, car il ne fait l'objet d'aucune définition légale ou réglementaire (12) ; tout du moins, ne fait-il pas l'objet d'une définition universelle de la part des États, chacun ayant tenté d'appréhender cette notion selon ses propres critères. Ce constat a induit la doctrine à multiplier les définitions de ce terme conduisant irrémédiablement à rendre plus complexes les analyses juridiques.

Au niveau national : la cybercriminalité n'est pas saisie par le droit interne, même s'il y est fait référence, la seule occurrence dans un code se trouve à l'article 694-32 du Code de procédure pénale déterminant la liste des infractions pour lesquelles le mandant d'arrêt européen de l'article 695-23 du même code peut être exécuté sans le contrôle de la double incrimination (Décision-cadre du

13 juin 2002 (13), art. 695-23 du code de procédure pénale) et, par renvoi à cette dernière disposition, pour les échanges européens relatifs au gel des avoirs (Décision-cadre du 22 juillet 2003 (14), art. 695-9-3 et 695-9-17 du même code), aux sanctions pécuniaires (Décision-cadre du 24 février 2005 (15), art. D. 48-24 du même code), aux confiscations (Décision-cadre du 06 octobre 2006 (16), art. 713-2 et 713-20 du même code), aux informations (Décision-cadre du 18 décembre 2006 (17), art. 695-9-38 et R. 49-36 du même code), et aux peines privatives de liberté (Décision-cadre du 27 novembre 2008 (18), art. 728-27 du même code). Pourtant, certaines lois consacrent des développements particuliers à la lutte contre la cybercriminalité, telle la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ou la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.

Selon le Ministère de l'intérieur français, la cybercriminalité recouvre « *l'ensemble des infractions pénales susceptibles de se commettre sur les réseaux de télécommunication en général et plus particulièrement sur les réseaux partageant le protocole TCP-IP, appelés communément l'Internet* » (19). Cependant, cette définition adoptée par le Ministère de l'intérieur français vise seulement les infractions dirigées contre les réseaux de télécommunications. Elle ne recouvre ni les infractions susceptibles d'être commises sur les systèmes informatiques, ni les infractions directement générées par le fonctionnement des réseaux informatiques. Il s'agit des infractions portant sur l'information véhiculée par le système informatique comme l'escroquerie, l'abus de confiance, et les atteintes aux libertés individuelles par la création illicite de fichiers nominatifs. Donc, l'absence de définition légale précise n'est pas sans poser de problèmes dans ce pays.

Au niveau européen : Il existe de nombreuses définitions de la cybercriminalité au niveau européen. Leur point commun est qu'elles comportent d'une part les faits de criminalité ciblant des ordinateurs et des systèmes d'information, et d'autre part les faits de criminalité commis à partir d'un ordinateur. Mais la législation européenne ne mentionne pas explicitement la cybercriminalité et elle ne fait que quelques allusions comme dans la décision d'Interpol ou l'article 83 du traité sur le fonctionnement de l'Union européenne (20) à la criminalité informatique (21). Il s'agit d'une volonté des politiques européennes de ne pas restreindre le phénomène par une définition trop étroite qui pourrait exclure des comportements qui ne sont pas identifiés comme de la cybercriminalité au regard de son apparition récente.

La Commission européenne définit la cybercriminalité dans un sens large comme « *toute infraction qui implique l'utilisation des technologies informatiques* ». La commission européenne s'est expliquée dans une communication au parlement européen en date du 22 mai 2007 (22) « *Faute d'une définition communément admise de la criminalité dans le cyberespace, les termes « cybercriminalité », « criminalité informatique » ou « criminalité liée à la haute technologie » sont souvent utilisés indifféremment* ». La Commission européenne, dans la communication précitée, précisait que « *la cybercriminalité devait*

s'entendre comme des infractions pénales commises à l'aide de réseaux de communications électroniques et de systèmes d'informations ou contre ces réseaux et systèmes ».

Au niveau international : Il n'y a aucun accord sur le point de savoir où commence et où finit la spécificité de la criminalité informatique. La preuve est qu'il n'y a pas d'homogénéité dans l'appellation de ce phénomène. On parle de délinquance, de criminalité, d'infraction, de fraude, de délit informatique, de « computer abuse », de cyberdélits ou de cybercrimes. Le fait que la criminalité et la délinquance relèvent du droit pénal des nations engendre de multiples définitions, caractéristiques ou typologies du crime informatique, variables selon les pays. Il apparaît difficile de trouver une certaine cohésion dans la définition de cette nouvelle forme de criminalité. Malgré l'inexistence d'une définition universelle de la criminalité informatique (23), seuls deux textes internationaux évoquent explicitement la cybercriminalité dans leurs intitulés : la Convention de Budapest sur la cybercriminalité du 23 novembre 2001 (24), et son protocole additionnel du 28 janvier 2003, sans aucune définition précise ne lui a été consacrée. Cette restriction des définitions semble pourtant trouver une double justification. D'abord, il est toujours difficile de définir un phénomène criminel lorsque celui-ci est nouveau. En l'espèce, la cybercriminalité est un fléau trop récent pour qu'une quelconque autorité dispose du recul nécessaire permettant de définir précisément ce type de délinquance. L'intérêt de l'article unique de la convention est de définir clairement les caractéristiques de la cybercriminalité telle le système informatique ou les données informatiques sans définir le phénomène lui-même (25). Dans cet article, Il est possible de trouver quelques pistes : « *Convaincus de la nécessité de mener, en priorité, une politique pénale commune destinée à protéger la société de la criminalité dans le cyberespace, notamment par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale* ». Ce texte conduit ainsi à proposer la définition suivante : la cybercriminalité est « *la criminalité dans le cyberespace* ». Cette définition de la cybercriminalité ne semble toutefois conduire qu'à d'autres difficultés : s'agissant d'une criminalité d'emprunt, celle-ci se fonde nécessairement sur la souveraineté des différents systèmes juridiques ; souveraineté fondée sur des frontières territoriales qui sont inconnues du cyberespace. Dès lors, assujettir la cybercriminalité aux règles de compétence territoriale entraîne des difficultés, tant sur le fond qu'au niveau procédural (26). La seconde justification semble porter sur la crainte de restreindre la matière. En effet, le comité des ministres a anticipé la commission d'infractions, encore inconnues, dans le cyberespace. La conséquence d'une définition juridique précise d'une délinquance émergente serait d'enfermer la notion sans pouvoir intégrer de nouvelles infractions, inconnues jusqu'alors.

De par sa dimension internationale, la cybercriminalité a suscité une réaction de certaines instances officielles qui ont tenté de surmonter cette difficulté, d'abord en visant le traitement, la transmission ou la sécurité de données (27) ; ensuite, en faisant référence à l'ordinateur ou au système informatique comme objet ou comme instrument de la cybercriminalité ; d'autres

définissent la cybercriminalité au regard d'un système informatique connecté à un réseau (28) ; d'autres enfin, se focalisent sur le caractère non autorisé de l'accès à un ordinateur, à un réseau ou à des fichiers à données électroniques (29).

Un point commun essentiel unit l'ensemble de ces définitions : le fait que le mode de commission de l'infraction se fasse à distance, sans contact physique entre l'auteur et la victime. En effet, il faut déduire de ces développements que l'absence de définition juridique précise est bien une volonté des États et non le signe d'une impuissance des acteurs à définir la notion. Même si cela peut paraître contraignant, les arguments évoqués par les autorités compétentes sont justifiés. En effet, le principal objectif poursuivi par les États est clairement de ne pas restreindre le contenu de la matière qui risque d'évoluer, de se modifier avec le temps en raison du caractère trop récent de ce fléau. Néanmoins, cette absence de définition juridique volontaire entraîne également des conséquences négatives quant à la répression déjà existante.

2- La difficulté à cerner le champ d'application de cette criminalité

La difficulté d'appréhender la criminalité sur le réseau tient tout d'abord au fait que l'Internet étant un moyen de communication et d'information mondial permettant de véhiculer tous les types de données (images, textes, chiffres) qui rendent de moins en moins visible une hiérarchisation de ces infractions, tant au niveau de leur nature juridique qu'au niveau de leur gravité. Le terme de cyberdélit a donc été utilisé pour décrire une grande variété d'infractions.

Parler de la cybercriminalité est assez délicat, puisqu'il s'agit d'une notion émergente et complexe. Cette notion est polymorphe, caractérisée par les technologies utilisées, car elle peut concerner aussi bien des infractions classiques ou conventionnelles commises par le biais d'Internet, que de nouvelles infractions nées de l'essence même de cet outil informatique. La cybercriminalité englobe, en fait, deux catégories d'infractions pénales :

Les infractions liées aux Technologies de l'Information et de la Communication qui s'appuient sur la nature des technologies utilisées. Cette criminalité regroupe les infractions pour lesquelles les télécommunications, la téléphonie cellulaire ou l'informatique sont l'objet même du délit. À titre d'exemple, les infractions de la délinquance informatique, incriminées par la loi du 5 janvier 1988 dite Godfrain, reprise dans les articles 323-1 et suivants du Code pénal, ont trait soit aux Systèmes de Traitement Automatisé de Données, soit à la confidentialité, à l'intégrité ou à la disponibilité des données d'information. Cette catégorie d'infractions impose une mise à jour des définitions des infractions dans les codes pénaux nationaux.

Et la criminalité spécifiquement véhiculée ou commise par Internet qui concerne une délinquance de droit commun, de nature juridique traditionnelle, mais qui tend à prendre une dimension particulière du fait des caractéristiques du réseau des réseaux (30).

Le point commun de ces catégories d'infractions est que celles-ci peuvent être commises à grande échelle et que la distance géographique entre le lieu

de commission de l'acte délictueux et ses effets peut être considérable. Le droit du numérique est aujourd'hui un véritable millefeuille législatif et règlementaire (31). Il est donc peu aisé, autant pour les professionnels que pour les profanes, de connaître avec précision ce qui est aujourd'hui reconnu comme un acte cyber criminel par le droit français (32). La conséquence de cette forte activité législative a pourtant été une trop grande accumulation des textes générant de multiples modifications et renvois qui, au lieu de simplifier, ont rendu compliqué la lutte contre la cybercriminalité.

3- Cybercriminalité : une délinquance difficile à mesurer

Les statistiques policières et judiciaires seraient impuissantes à rendre compte des cyber-infractions ne donnant lieu ni à plainte, ni à dénonciation, ni à saisine d'office.

La faible propension des victimes à déposer une plainte : nombreuses sont les personnes qui se retrouvent escroquées ou usurpées dans leur identité par un cyberdélinquant sans même le savoir ou à l'inverse avec le savoir quand elles tentaient d'acheter un produit illégal ou contrefait sur un site étranger ne portera pas plainte car comme le dit l'adage « *nul ne peut se prévaloir de sa propre turpitude* ». De plus, la victime n'est pas toujours consciente du geste criminel commis à son égard. Par exemple, une personne reçoit des insultes en ligne peut décider que les actions du harceleur ne sont pas assez sérieuses pour être qualifiées de crime et retenir ainsi l'attention de la police. Ainsi, certaines victimes peuvent avoir honte d'être tombées dans un piège tendu par autrui. Les fraudes nigérianes sont des exemples de cas où les victimes peuvent hésiter à révéler leur victimisation de peur de subir un jugement négatif. Quant aux fraudes à la carte bancaire, les détenteurs sont indemnisés par le système bancaire sans devoir justifier d'une plainte préalable. S'agissant enfin des professionnels de l'Internet, leur obligation de dénonciation est aujourd'hui cantonnée à quelques infractions graves. Au surplus, nombre de cyber-délits sont "transparents" pour l'utilisateur qui peut ignorer son état de victime ou s'en apercevoir longtemps après. Si la technique des signalements par les internautes, notamment ceux adressés directement à l'État (la plate-forme PHAROS), permet de pallier, dans une certaine mesure, cette méconnaissance, il n'est pas possible d'en mesurer exactement l'impact. En retour, cela affecte la capacité de la police à produire un portrait statistique du phénomène fidèle à la réalité. Donc l'une des principales difficultés auxquelles doivent faire face les services de police est d'obtenir la coopération des victimes.

La non-dénonciation d'une infraction par les personnes morales : Tout comme la personne, l'entreprise privée n'est pas encline à divulguer sa victimisation à la police. Dans le milieu des affaires, de sérieux doutes planent quant à la capacité de la police publique à effectuer des enquêtes informatiques efficaces, rapides et confidentielles (33). L'une des craintes premières des institutions est que l'enquête policière exposera publiquement la négligence de l'entreprise en matière de sécurité. Elles ne sont pas persuadées de l'intérêt de la démarche de dénonciation du délit (espoir faible d'obtenir réparation, doute sur

l'aide effective qui pourrait être apportée durant une période de crise, sur la réactivité des instances judiciaires) ; elles pensent que la démarche est complexe, lourde, onéreuse, consommatrice d'énergie, de temps, de ressources, alors que les entreprises sont focalisées sur la résolution de l'incident afin d'assurer la continuité des services (34). Elles préfèrent faire justice elles mêmes, ce qui est illégal, en piratant à leur tour le ou les systèmes impliqués dans l'attaque dont elles ont été victimes (35).

Les méthodes d'évaluation des coûts : Les méthodes d'évaluation des coûts directs et indirects de la cybercriminalité peuvent également être variables. Certaines études calculent par exemple uniquement la mise en place de systèmes de sécurité et la réparation des dommages directs à la suite d'une attaque, tandis que d'autres recherches incluront les coûts indirects des attaques comme le manque à gagner causé par la perte de clients.

Il y a donc des difficultés à établir des statistiques précises des faits de cybercriminalité. Premièrement, les statistiques sur la criminalité sont généralement établies au niveau national et ne reflètent pas l'étendue du phénomène au niveau international. Alors qu'il serait possible de combiner les données provenant de différents États, cette approche ne produirait pas d'informations fiables en raison des différences entre les législations. Deuxièmement, les statistiques ne peuvent rendre compte que des infractions qui ont été constatées et signalées (36). S'agissant de la cybercriminalité en particulier, le nombre de cas non signalés pourrait être élevé.

Les conséquences du flou définitionnel d'une délinquance émergente

Le flou définitionnel entourant la notion de cybercrime entraîne plusieurs problèmes quant à la collaboration et à l'élaboration de plans d'action. Sans un langage commun, il est difficile de parvenir à diriger l'action vers les bonnes cibles. Sans consensus sur la définition, il devient ardu d'obtenir des statistiques universelles sur le phénomène et de produire ainsi une image claire de la déviance sur Internet (37). Cette absence de définition légale a aussi des effets néfastes, car de ce fait, certains magistrats ne cernent pas encore l'ampleur du phénomène et les préjudices réels qui en découlent et cela continue à profiter aux délinquants agissant par le biais des nouvelles technologies.

L'absence de définition légale de la cybercriminalité est en soi une faiblesse du droit français dans la lutte contre celle-ci. Une définition du terme s'impose alors dans le Code pénal, d'autant plus que la cybercriminalité tend à s'amplifier avec le développement technologique. Le nombre des infractions se dématérialisent et de plus en plus, se démultiplient, se simplifient et se diversifient et les délinquants se jouent des frontières en commettant leurs délits dans des pays où la législation est inexistante ce qui aboutit à la création de cyberparadis.

La cybercriminalité est devenue une préoccupation majeure pour les organisations gouvernementales et du secteur privé, et elle donne lieu à une multi-

plication des études, que ce soit dans le domaine informatique, juridique ou criminologique. Malgré une croissance exponentielle de ce phénomène, sa notion demeure encore lacunaire et hétérogène. À l'heure actuelle, il n'a pas en effet atteint un consensus sur la signification de la cybercriminalité, chaque État ayant défini cette notion selon ses propres critères (38). Ce flou terminologique est renforcé par l'absence d'un cadre législatif uniforme définissant la cybercriminalité. Pour faire face à ce déficit, la création d'un Code pénal international pourrait constituer une réponse adaptée (39).

A. La nécessaire élaboration d'un droit commun de l'Internet

L'Internet est une société virtuelle où chacun se côtoie sans se connaître vraiment. Pourtant les échanges y sont extraordinairement importants. En outre, il présente le précieux avantage d'abolir les frontières, réduisant ainsi l'inconvénient des distances. Comment serait-il donc possible dans ces conditions de ne pas apporter à ce nouveau genre de société un cadre juridique qui soit en parfaite adéquation avec son internationalisme ? Il pourra facilement répondre à cette question en se plaçant d'abord sur le plan de la légitimité d'un droit commun de l'Internet avant d'envisager son indéniable efficacité.

1- Légitimité d'un droit commun de l'Internet

Un État n'est de droit que s'il est réellement légitime. Aussi s'il s'en tient à la définition de la légitimité il rappellera qu'il faut entendre par là : la qualité d'un pouvoir d'être conforme aux aspirations des gouvernés, ce qui lui vaut l'assentiment général et l'obéissance spontanée. Or, la légitimité n'est pas par essence une valeur préexistante au sein d'un État et elle n'est pas immuable. La difficulté réside dans l'adhésion au plus grand nombre à des valeurs communes. Or, force est de constater que cette adhésion au plus grand nombre n'est réalisable qu'à partir du moment où il existe au sein d'un groupe, d'une communauté, ou d'une nation, un sentiment d'appartenance à cette entité quelle qu'elle soit. Il faut pour cela qu'il existe une certaine cohésion afin d'établir à partir de valeurs communes un système juridique pouvant emporter l'assentiment général et l'obéissance spontanée. C'est à partir de là que l'on a créé les nations, les États. La source de la légitimité d'un État et de ses règles se trouve dans chacun des hommes et des femmes qui y ont élu domicile et adhérant dans l'ensemble à un même mode de vie. Néanmoins, il convient de relever que la situation n'est pas aussi angélique qu'il y paraît puisque la légitimité d'un système connaît ses limites dans le sens où les hommes au-delà du sentiment d'appartenance à un même État n'en demeurent pas moins différents les uns des autres. Pourtant au-delà des clivages religieux, politiques, ethniques ou culturels, il a toujours été plus aisé d'élaborer des règles de droit dans un cadre strictement national. En effet, les clivages internes apparaissent en général moins importants que les clivages pouvant exister entre deux États. Dans ces conditions, le système de droit interne justifie de plus de légitimité. Mais à ce jour et avec l'arrivée de l'Internet, il est fondamental que le droit de l'Internet puisse s'élaborer entre tous les États, au-delà des différences culturelles, et afin

de tendre à une légitimité commune c'est-à-dire une légitimité entendue non plus sur la scène juridique nationale, mais sur la scène internationale. L'Internet ne peut se contenter d'une légitimité purement étatique, elle se doit d'emporter la conviction de chaque pays. C'est précisément sur cette légitimité qu'il est difficile de travailler. Pourtant c'est en apportant cette légitimité commune que le droit de l'Internet sera efficace et par la même capable de lutter contre la cybercriminalité.

2- L'efficacité d'un droit commun de l'Internet

Le droit applicable à l'Internet ne peut être efficace dans sa lutte contre les déviances s'il se cantonne à l'application pure et simple du droit interne. En effet, puisque l'Internet est un outil évoluant en dehors de toute frontière étatique, il convient d'élaborer un droit commun permettant ainsi une meilleure répression des infractions perpétrées via le Net. Cela passe par une collaboration étroite entre les autorités concernées par la régulation de l'Internet mais aussi entre les acteurs directs de la Toile à savoir les utilisateurs eux-mêmes (particuliers et entreprises). Si le Conseil d'État faisait remarquer dans son rapport de 1998 (40) qu'il n'était nul besoin de développer une législation spécifique à l'Internet, cela était sans compter sur les nombreux conflits de lois pouvant intervenir en la matière et principalement quant à la question de la cybercriminalité. En effet, il est évident que les États doivent pouvoir compter sur une collaboration étroite entre tous les pays afin de lutter efficacement contre le phénomène de la cybercriminalité. Cela implique donc la mise au point de règles spécifiques de procédure permettant de faciliter les enquêtes sans porter atteinte à la souveraineté des États. Mais le problème est plus ardu qu'il n'y paraît puisque à l'évidence ce qui pourra être toléré dans un pays ne le sera pas forcément dans le pays voisin. Conscient de la nécessité de développer un droit international de l'Internet et de se doter de moyens efficaces permettant de réduire la criminalité du Net, le Conseil de l'Europe tente d'apporter depuis plusieurs années des réponses précises aux nombreux problèmes juridiques soulevés par l'Internet. Cette régulation s'articule autour de plusieurs thèmes et notamment celui de la cybercriminalité. Pour être efficace et favoriser le développement de la société de l'information, il apparaît fondamental que les États travaillent ensemble afin de faciliter la lutte contre la cyberdélinquance qui représente un réel fléau tant le préjudice financier est important. Pourtant si les États ont dans l'ensemble compris l'intérêt qu'il y avait à coopérer, il n'en demeure pas moins que les négociations ne sont pas une mince affaire tant les écarts culturels peuvent être importants.

B. Les difficultés d'élaboration d'un droit commun de l'Internet

Alors que les textes foisonnent depuis une dizaine d'années, force est de constater que l'Internet ne fait pas l'objet d'une législation spécifique. Cette absence de texte n'est pas aussi préjudiciable qu'on pourrait le penser. En effet, il faut relever que l'évolution rapide des nouvelles technologies prendrait la loi en défaut, et toute réaction du législateur aboutirait à un système juridique

manquant de stabilité. Aussi fait-il relever que deux éléments caractéristiques majeurs pèsent lourdement sur les possibilités de régulation de l'Internet : d'une part le caractère universel du Net et, d'autre part, la diffusion multiforme de l'information.

L'internationalisation implique d'admettre l'inefficacité du système judiciaire français en l'État et personnalise la répression de la cybercriminalité, détachée de celle de la délinquance véhiculée ou commise sur un support non électronique. Cette vision a pour effet de nier la nature juridique traditionnelle de la cybercriminalité au profit d'une conception nouvelle de la criminalité définie au regard des caractéristiques de son support ou moyen de commission. D'autre part, l'existence de cet arsenal juridique mondial, tant sur un plan législatif que procédural et judiciaire s'inscrit dans une prise en considération des principes fondateurs de chaque pays touché par la cybercriminalité. Cela revient à faire coexister des centaines de principes divergents au sein d'un même système judiciaire. Ce qui est, aujourd'hui, à l'évidence, utopique. L'existence d'un tel système judiciaire mondial, fondé sur des principes fondamentaux propres, obligerait chaque État à abandonner un certain nombre de leurs spécificités historiques, culturelles et juridiques ; abandon qui entraînerait des risques d'incompréhension voire de rejet des peuples concernés. En France, le code des postes et des télécommunications réglemente les télécommunications traditionnelles. Cependant, il ne s'agit pas d'une loi unique mais d'un ensemble de textes réunis au sein d'un même code. Ainsi, ce code est principalement axé sur l'aspect transport des communications. Quant à leurs contenus, ils sont régis par un ensemble de textes variant en fonction de leur nature : propriété des contenus (propriété intellectuelle et industrielle, protections des données nominatives), répression des contenus (applications des dispositions pénales). Une première solution fut donc avancée quant à la résolution de ces deux problèmes, à savoir l'autorégulation. Là encore les systèmes juridiques et les autorités étatiques peuvent être très différents. Ce qui sera toléré dans un pays ne le sera pas du tout dans un autre. Ainsi, il sera difficile de déterminer la loi applicable à l'Internet en cas de litige.

Conclusion

La cybercriminalité est une nouvelle forme de délinquance qui se commet généralement sur des réseaux informatiques, en particulier sur le réseau Internet. Grâce à la vulgarisation de ce dernier, non seulement des nouveaux actes antisociaux ont vu le jour, mais aussi des vieilles inconduites, déjà déplorées et réprimées dans différents systèmes pénaux, se sont perfectionnées. C'est ce polymorphisme qui constitue le particularisme de cette délinquance, et rend ambigüe toute tentative de sa conceptualisation : ni le législateur, ni la doctrine ne parviennent à contenir la cybercriminalité dans un cadre définitionnel précis pouvant permettre de cerner scientifiquement tous ses contours.

Bibliographie

AUROUX (J.-B.), « Nouvelles technologies de la communication électronique et droit pénal », *Revue Lamy Droit de l'Immatériel*, N° 15, 1er avril, 2006.

BÉNICHOU (D.), « Cybercriminalité : jouer d'un nouvel espace sans frontière », *AJ pénal*, 2005.

BERTHELET (P.), « Aperçus de la lutte contre la cybercriminalité dans l'Union européenne », *RSC*, 2018, p. 59.

BOYER (B.), *Cyberstratégie, l'art de la guerre numérique*, édition Nuvis, 2012.

BUTTARELLI (G.), *Vers la création du Centre européen de lutte contre la cybercriminalité (EC3) au sein d'Europol : quelles sont les implications en matière de protection des données ?*, Séminaire de l'EER Bruxelles le 16 mai 2012.

CAZANEUVE (J.), « La cybercriminalité : l'émergence d'un nouveau risque », *AJ pénal*, 2012.

CHAWKI (M.), « Essai sur la notion de cybercriminalité », *IEHEI*, 2006.

CHOPIN (F.), *Cybercriminalité*, Répertoire de droit Pénal et de procédure pénale, 2015.

Communication de la Commission des communautés européennes au parlement européen, au Conseil et au comité des régions, *Vers une politique générale en matière de lutte contre la cybercriminalité*, 22 mai 2007, COM (2007) 267 final.

Congrès annuel des Nations Unies à Vienne relatif à la prévention du crime et le traitement des délinquants qui s'est déroulé du 10 au 17 avril 2000.

Conseil de l'Europe, *Criminalité organisée en Europe : la menace de la cybercriminalité*, éditions du Conseil de l'Europe, 2006.

Convention sur la cybercriminalité du Conseil de l'Europe signée à Budapest le 23 nov. 2001, entrée en vigueur le 1er juillet 2004, V. site du Conseil de l'Europe : www.coe.int.

Décision-cadre 2003/577/JAI du Conseil du 22 juillet 2003 relative à l'exécution dans l'Union européenne des décisions de gel de bien ou d'éléments de preuve, Journal Officiel de l'Union européenne L. 196/45 du 02 août 2003.

Décision-cadre 2005/214/JAI du Conseil du 24 février 2005 concernant l'application du principe de reconnaissance mutuelle aux sanctions pécuniaires, Journal Officiel de l'Union européenne L. 76/16 du 22 mars 2005.

Décision-cadre 2006/783/JAI du Conseil du 6 octobre 2006 relative à l'application du principe de reconnaissance mutuelle aux décisions de confiscation, Journal Officiel de l'Union européenne L. 328/59 du 24 novembre 2006.

Décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des Etats membres de l'Union européenne, Journal Officiel de l'Union européenne L. 386/89 du 29 décembre 2006.

Décision-cadre 2008/977/JAI du conseil du 27 novembre 2008relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judicaire en matière pénale, Journal Officiel de l'Union européenne L. 350 du 30 décembre 2008.

Décisions-cadre 2002/584/JAI du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre Etats membres, Journal Officiel des Communautés européennes L. 190/1du 18 juillet 2002.

DJOGBENOU (J.), cybercriminalité-enjeux et défis pour le bénin, projet de renforcement des capacités en conception et analyse des politiques de développement PDF, Document N° 007/2010.

FORTIN (F.), *Cybercriminalité : entre inconduite et crime organisé*, édition les Presses internationales polytechnique, collection Pro'Didakt, 2013.

GHERNAOUTI-HÉLIE (S.), *La cybercriminalité : le visible et l'invisible*, éditions Presses polytechniques et universitaires romandes, collection Le Savoir Suisse, 2009.

GHERNAOUTI-HÉLIE (S.), *Sécurité informatique et réseaux*, 4e édition, DUNOD, 2013.

Traité sur le Fonctionnement de l'Union Européenne

KABAY (M.-E.), "Understanding Studies and Surveys of Computer Crime", 2013, disponible à l'adresse : http://www.mekabay.com/methodology/crime_stats_methods.pdf.

Ministère de l'Intérieur français, « Qu'est-ce-que la cybercriminalité ? », 2012, accessible en ligne à http://www.interieur.gouv.fr/A-votre-service/Ma-securite/Conseils-pratiques/Sur-Internet/Qu-est-ce-que-la-cybercriminalite (site consulté le 23/02/2013).

Ministère de la justice, « La nécessité d'une réponse coordonnée », 27 juin 2011, http://www.justice.gouv.fr/justice-penale-11330/cybercriminalite-la-necessite-dune-reponse-coordonnee-22472.html.

PRATES (F.) et GAUDREAU (F.) et DUPONT (B.), « La cybercriminalité : état des lieux et perspectives d'avenir », Publié dans : Institut Canadien d'Études Juridiques Supérieures (sous la direction de), *Droits de la personne : La circulation des idées, des personnes et des biens et capitaux*, Éditions Yvon Blais, Cowansville, 2013, http://www.benoitdupont.net/sites/www.benoitdupont.net/files/Prates%20Gaudreau%20Dupont%202013%20cybercriminalit%C3%A9.pdf.

PRZYSWA (E.), *Cybercriminalité et contrefaçon*, édition FYP, 2010.

QUEMENER (M.) et CHARPENEL (Y.), *Cybercriminalité ; droit pénal appliqué*, Économica, 2010.

QUÉMÉNER (M.) et CHARPENEL (Y.), « La justice face à la cybercriminalité », *Revue de la gendarmerie nationale*, 4° trimestre, n° 244, 2012.

QUÉMÉNER (M.) et FERRY (J.), *Cybercriminalité : défi mondial*, 2ème édition, Economica, 2009.

QUEMENER (M.), « Le rôle préventif de la justice en matière de cybersécurité », *Dalloz IP/IT*, 2016.**Rapport du Conseil d'État**, *Internet et les réseaux numériques*, Collection études du conseil d'État, La documentation française, 1998.

Résolution du Parlement européen du 3 octobre 2017 sur la lutte contre la cybercriminalité (2017/2068(INI)).

Notes

1 Cette méthode d'adaptation réalisée n'est pas sans inconvénient, créant ainsi un éparpillement dans différents codes notamment : Code pénal, Code des postes et des communications électroniques, Code de la sécurité intérieure, Code de la défense, et enfin, un risque d'obsolescence des dispositions pénales.

2 Considération.M de la résolution du Parlement européen du 3 octobre 2017 sur la lutte contre la cybercriminalité (2017/2068(INI)).

3 L'immatérialité de son objet (cyberespace) qui n'a jamais finalisé, il reste toujours ouvert à l'expansion. C'est la réplique réelle mais immatérielle et numérique de notre monde physique avec ses villes constituées de serveurs, ses maisons et immeubles que sont les ordinateurs, les téléphones portables et tous autres gadgets permettant de rester connecté, ses axes de circulations permettant l'information de circuler et d'être consultée à partir ne n'importe quel endroit sur terre, ses moyens de reconnaissance que sont les adresses IP, les URL, les adresses mails et ses habitants que sont les internautes qui ne marchent ni ne roule comme nous mais surfent :http://www.droit-technologie.org/dossier-230/la-repression-de-la-cybercriminalite-en-droit-senegalais-a-l-epreuve-d.html.

4 La transnationalité des réseaux qui permet au criminel de pouvoir commettre une infraction de n'importe quel endroit de son choix, de sorte que les éléments de l'infraction peuvent se retrouver dispersés sur les territoires de plusieurs pays dont les législations ne seront pas forcément homogènes avec d'inévitables problèmes de conflits de souveraineté.

5 La facilité du recours de l'anonymat sur les réseaux, qui rend difficile la localisation et l'identification des auteurs, indispensables pour permettre l'imputabilité des infractions.

6 Le caractère dynamique et évolutif de cette criminalité qui se développe aussi rapidement que les nouvelles technologies, prenant ainsi en défaut le principe de prévisibilité du droit pénal. Également, la rigidité du principe de légalité qui limite le pouvoir d'interprétation devient un obstacle à la réactivité de la répression.

7 La fragilité et volatilité des éléments constitutifs des infractions qui peuvent être effacés ou modifiés à tout moment et de n'importe quel endroit, et qui doivent donc être préservés rapidement pour permettre aux services d'enquête et de poursuites de caractériser l'infraction, J. DJOGBENOU, cybercriminalité-enjeux et défis pour le bénin, projet de renforcement des capacités en conception et analyse des politiques de développement PDF, Document N° 007/2010, p. 11.

8 P. BERTHELET, « Aperçus de la lutte contre la cybercriminalité dans l'Union européenne », *RSC*, 2018, p. 59.

9 Conseil de l'Europe, *Criminalité organisée en Europe : la menace de la cybercriminalité*, éditions du Conseil de l'Europe, 2006, p. 225.
10 E. PRZYSWA, *Cybercriminalité et contrefaçon*, édition FYP, 2010, p. 1.
11 F. CHOPIN, *Cybercriminalité*, Répertoire de droit Pénal et de procédure pénale, 2015.
12 M. CHAWKI, « Essai sur la notion de cybercriminalité », *IEHEI*, 2006, p. 6.
13 Décisions-cadre 2002/584/JAI du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre Etats membres, Journal Officiel des Communautés européennes L. 190/1du 18 juillet 2002.
14 Décision-cadre 2003/577/JAI du Conseil du 22 juillet 2003 relative à l'exécution dans l'Union européenne des décisions de gel de bien ou d'éléments de preuve, Journal Officiel de l'Union européenne L. 196/45 du 02 août 2003.
15 Décision-cadre 2005/214/JAI du Conseil du 24 février 2005 concernant l'application du principe de reconnaissance mutuelle aux sanctions pécuniaires, Journal Officiel de l'Union européenne L. 76/16 du 22 mars 2005.
16 Décision-cadre 2006/783/JAI du Conseil du 6 octobre 2006 relative à l'application du principe de reconnaissance mutuelle aux décisions de confiscation, Journal Officiel de l'Union européenne L. 328/59 du 24 novembre 2006.
17 Décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des Etats membres de l'Union européenne, Journal Officiel de l'Union européenne L. 386/89 du 29 décembre 2006.
18 Décision-cadre 2008/977/JAI du conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judicaire en matière pénale, Journal Officiel de l'Union européenne L. 350 du 30 décembre 2008.
19 Ministère de l'Intérieur français, « Qu'est-ce-que la cybercriminalité ? », 2012, accessible en ligne à http://www.interieur.gouv.fr/A-votre-service/Ma-securite/Conseils-pratiques/Sur-Internet/Qu-est-ce-que-la-cybercriminalite (site consulté le 23/02/2013).
20 L'article 83 paragraphe 1 du Traité sur le Fonctionnement de l'Union Européenne prévoit que « *l'EU peut adopter des directives établissant des règles minimales concernant la définition des infractions pénales, à condition que cela concerne des domaines de criminalité particulièrement graves revêtant une dimension transfrontalière, tels que le terrorisme, la traite des êtres humains et l'exploitation sexuelle des femmes et des enfants, le trafic illicite de drogues, le trafic illicite d'armes, le blanchiment d'argent, la corruption, la contrefaçon de moyens de paiement, la criminalité informatique et la criminalité organisée* ».
21 G. BUTTARELLI, *Vers la création du Centre européen de lutte contre la cybercriminalité (EC3) au sein d'Europol : quelles sont les implications en matière de protection des données ?*, Séminaire de l'EER Bruxelles le 16 mai 2012.
22 Communication de la Commission des communautés européennes au parlement européen, au Conseil et au comité des régions, *Vers une politique générale en matière de lutte contre la cybercriminalité*, 22 mai 2007, COM (2007) 267 final, p. 2.
23 J. CAZANEUVE, « La cybercriminalité : l'émergence d'un nouveau risque », *AJ pénal*, 2012, p. 268) ; M. QUEMENER, « Le rôle préventif de la justice en matière de cybersécurité », *Dalloz IP/IT*, 2016, p. 12 ; M. QUEMENER et Y. CHARPENEL, *Cybercriminalité ; droit pénal appliqué*, Économica, 2010.
24 Convention sur la cybercriminalité du Conseil de l'Europe signée à Budapest le 23 nov. 2001, entrée en vigueur le 1er juillet 2004, V. site du Conseil de l'Europe : www.coe.int.
25 D. BÉNICHOU, « Cybercriminalité : jouer d'un nouvel espace sans frontière », *AJ pénal*, 2005, p. 224.
26 J.-B. AUROUX, « Nouvelles technologies de la communication électronique et droit pénal », *Revue Lamy Droit de l'Immatériel*, N° 15, 1er avril, 2006.
27 Pour l'OCDE, la cybercriminalité renvoie 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* » définition citée par S. GHERNAOUTI-HÉLIE, *La cybercriminalité : le visible et l'invisible*, éditions Presses polytechniques et universitaires romandes, collection Le Savoir Suisse, 2009, p. 22 ; pour l'ONU, elle a trait à « *tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent* » Définition établie

lors du Xème Congrès annuel des Nations Unies à Vienne relatif à la prévention du crime et le traitement des délinquants qui s'est déroulé du 10 au 17 avril 2000 ; de telles définitions, trop partielles, ne couvrent toutefois pas l'ensemble des infractions concernées, telles la pédopornographie. La définition proposée par l'ONU met en avant « le comportement illégal » pour se référer à la cybercriminalité, mais un comportement peut être illégal dans un pays et licite dans un autre.

28 C'est le plus grand nombre.

29 Telle est la définition donnée par les U.S.A. et le Royaume-Uni ; mais se focaliser sur l'accès ne permet pas de rendre compte de toute la cybercriminalité, ne serait-ce que lorsqu'elle prend la forme d'une diffusion de données ou de comportements illicites.

30 Elle est constituée par les crimes et délits à l'encontre des personnes et des biens tels que les dénonciations calomnieuses incriminées à l'article 226-10 du Code pénal ; la diffusion, la fixation, l'enregistrement ou la transmission d'images à caractère pornographique d'un mineur visés à l'article 227-13 du Code pénal ou les escroqueries réprimées par l'article 313-1 du Code pénal. Elle vise également les infractions incriminées par des textes spécifiques telles que les infractions relatives à la loi sur la presse du 29 juillet 1881, les infractions au Code de la propriété intellectuelle, les infractions à la loi du 29 décembre 1990 sur les règles de cryptographie, les infractions à la loi du 12 juillet 1983 sur la participation à une maison de jeu ou encore les infractions au Code de la santé publique.

31 M. QUÉMÉNER et Y. CHARPENEL, « La justice face à la cybercriminalité », *Revue de la gendarmerie nationale*, 4° trimestre, n° 244, 2012 ; B. BOYER, *Cyberstratégie, l'art de la guerre numérique*, édition Nuvis, 2012, p. 104.

32 M. QUÉMÉNER et J. FERRY, *Cybercriminalité : défi mondial*, 2ème édition, Economica, 2009, p. 6.

33 F. FORTIN, *Cybercriminalité : entre inconduite et crime organisé*, édition les Presses internationales polytechnique, collection Pro'Didakt, 2013, p. 16.

34 S. GHERNAOUTI-HÉLIE, *Sécurité informatique et réseaux*, 4e édition, DUNOD, 2013, p. 42.

35 S. GHERNAOUTI-HÉLIE, *La cybercriminalité : le visible et l'invisible*, éditions Presses polytechniques et universitaires romandes, collection Le Savoir Suisse, 2009, p. 61 et 62.

36 M.-E. KABAY, "Understanding Studies and Surveys of Computer Crime", 2013, disponible à l'adresse : http://www.mekabay.com/methodology/crime_stats_methods.pdf.

37 F. FORTIN, *cybercriminalité : entre inconduite et crime organisé*, précité, p. 15.

38 Ministère de la justice, « La nécessité d'une réponse coordonnée », 27 juin 2011, http://www.justice.gouv.fr/justice-penale-11330/cybercriminalite-la-necessite-dune-reponse-coordonnee-22472.html.

39 F. PRATES, F. GAUDREAU et B. DUPONT, « La cybercriminalité : état des lieux et perspectives d'avenir », Publié dans : Institut Canadien d'Études Juridiques Supérieures (sous la direction de), *Droits de la personne : La circulation des idées, des personnes et des biens et capitaux*, Éditions Yvon Blais, Cowansville, 2013, p. 5, http://www.benoitdupont.net/sites/www.benoitdupont.net/files/Prates%20Gaudreau%20Dupont%202013%20cybercriminalit%C3%A9.pdf.

40 Rapport du Conseil d'État, *Internet et les réseaux numériques*, Collection études du conseil d'État, La documentation française, 1998, p. 7.