

DE LA CYBERCRIMINALITÉ À LA CYBERGUERRE

Cybercriminalité : aspects stratégiques et juridiques

Myriam QUÉMÉNER

Internet et les réseaux numériques posent de nouveaux défis aux hommes qui doivent y avoir recours pour assurer leur développement économique, tout en se prémunissant et en luttant contre certaines dérives de leur utilisation criminelle et qui constitue désormais ce qu'on nomme la cybercriminalité. Les réseaux numériques sont en effet sources de nouvelles formes d'atteintes aux droits de la société et des individus qui nécessitent, en conséquence, une adaptation constante des réponses étatiques et législatives, des techniques et moyens policiers et judiciaires à la hauteur des préjudices humains et économiques subis. Les technologies de l'information et de la communication (TIC) apparaissent comme un vecteur idéal pour faciliter l'action des délinquants à commettre leurs multiples forfaits.

Les systèmes d'information constituent un important progrès pour nos sociétés, mais présentent aussi des risques et des vulnérabilités dont il est nécessaire de prendre conscience. Ainsi, depuis que l'*Internet* s'est développé dans le grand public, il ne se passe pas une semaine sans que les médias ne rapportent une affaire liée, de près ou de loin, à l'utilisation frauduleuse des réseaux. La croissance exponentielle des nouvelles techniques de communication dont *Internet* fait partie, a permis un transfert des activités traditionnelles du monde « réel » vers le « cyberspace », terme anglais créé par William Gibson dans son livre intitulé *Neuromancer*, parfois utilisé dans le sens de monde « virtuel ».

La population des internautes dans le monde devrait atteindre 1,5 milliard en 2011 soit 36 % de plus qu'en 2006 où leur nombre était estimé à 1,1 milliard. C'est dire les enjeux en termes d'atteintes aux personnes et aux biens qui nécessitent un traitement à la fois politique et législatif afin de préserver les sociétés.

CYBERCRIMINALITÉ, QUELLES RÉALITÉS ?

La cybercriminalité correspond à des facettes multiformes que l'on peut classer en deux catégories, d'une part les infractions où les systèmes informatiques sont l'objet même des actions répréhensibles, comme par exemple l'accès non autorisé aux données ou aux systèmes à des fins délictueuses ; et d'autre part les infractions telles la contrefaçon, les détournements de fonds, l'escroquerie, la détention et le recel de contenus illicites, la diffamation *via* des services en ligne, etc. La cybercriminalité fait référence aux activités criminelles qui s'effectuent, *via* les technologies et de l'*Internet* et à travers le cyberspace.

Il convient de protéger les réseaux contre des attaques informatiques qui peuvent prendre des formes diverses : *hacking* ⁽¹⁾, *cracking* ⁽²⁾ ou *phreaking* ⁽³⁾. Non seulement *Internet* offre des conditions exceptionnelles pour de nouvelles entreprises et activités illicites, mais il autorise également la réalisation de fraudes ou délits habituels *via* l'outil informatique. Ainsi, en favorisant la recherche et la production de revenus, *Internet* offre de nouvelles capacités au monde criminel. Une exploitation efficace des nouvelles technologies permet de réaliser des crimes économiques « classiques » tout en maximisant les bénéfices, le niveau de risque restant réduit. Les nouvelles technologies sont à considérer comme cible et comme moyen d'expression de nouvelles formes de criminalité. Avec le crime informatique, l'ordinateur peut être la finalité d'un délit, comme par exemple le vol ou la destruction de données, mais peut également servir d'intermédiaire pour perpétrer des activités délictueuses.

L'appréhension des comportements délictueux *via* les réseaux numériques se heurte à trois obstacles majeurs : l'anonymat qui séduit les délinquants ; la volatilité des informations numériques qui constitue un obstacle de taille en matière de recherche des preuves, celles-ci pouvant disparaître instantanément et le caractère transnational des comportements délinquants. Les enjeux sont multiples en matière de délinquance commise dans le cyberspace. Il conviendra d'évoquer tout d'abord les aspects stratégiques puis juridiques de la

(1) Piratage des réseaux.

(2) Attaque des protections des logiciels de programme.

(3) Sabotage ou prise de contrôle de centraux téléphoniques.

cybercriminalité qui s'adaptent en fonction de l'évolution des manifestations et des formes prises par ces dérives des temps modernes qui imposent des réponses nationales, mais aussi internationales.

LES ENJEUX STRATÉGIQUES DE LA CYBERCRIMINALITÉ

Il ne faut jamais oublier que l'étymologie de cyber, signifie en grec gouverner⁽⁴⁾, contrôler. Ce contrôle a naturellement plusieurs objectifs qui sont à la fois de nature politique, scientifique, culturelle et économique. En d'autres termes comme l'a rappelé Bernard Carrayon, député du Tarn, dans son rapport sur l'intelligence économique de juillet 2003 : « *Internet* est un véhicule à part entière de la dominance politique et stratégique des Nations qui le contrôlent »⁽⁵⁾. Il y a lieu de s'assurer que les réseaux informatiques globaux ne servent pas de support ou de vecteur à la préparation, à la commission ou à la dissimulation d'infractions pouvant atteindre des intérêts fondamentaux des États comme des entreprises.

On ne peut exclure des actions pouvant viser les États, comme l'encombrement de services vitaux ou la destruction concertée d'informations stratégiques et confidentielles. Par exemple le gouvernement estonien en a été victime en avril et mai 2007 : attaques informatiques massives contre ses principaux sites *Internet*, y compris ceux de plusieurs institutions gouvernementales et financières.

La sécurité des infrastructures d'information est devenue une préoccupation majeure des acteurs publics et privés qui mettent en place des parades technologiques et prennent des mesures pour lutter contre les contenus illicites ou préjudiciables sur *Internet*, protéger les droits de propriété intellectuelle et les données à caractère personnel, et renforcer la sécurité des transactions électroniques. Néanmoins, le nombre de virus s'est accru au cours de ces dernières années et ceux-ci deviennent de plus en plus sophistiqués. Les outils nécessaires aux pirates sont facilement accessibles en ligne et il existe un échange

(4) Tenir le gouvernail. Le verbe grec *kubernân* veut en effet dire piloter un navire ou un char et fut utilisé pour la première fois de façon métaphorique par Platon pour désigner le fait de gouverner les hommes. Il a donné naissance au verbe latin *gubernare*, qui revêt la même signification.

(5) www.bcarayon-ie.

Cybercriminalité : aspects stratégiques et juridiques

constant d'information et de savoir-faire entre les cybercriminels pour rendre les attaques de plus en plus efficaces. Les mesures de lutte contre les menaces doivent constamment s'adapter aux nouveaux comportements criminels. Le monde virtuel offre aux membres d'organisations criminelles un outil fiable, rapide, anonyme et peu onéreux.

On constate donc que les technologies de l'information sont devenues des armes stratégiques essentielles. On peut affirmer aujourd'hui que c'est suite à des actions terroristes que les États ont apporté de nombreux correctifs à leurs législations afin de déjouer les pièges des délinquants utilisant les réseaux numériques pour commettre leurs actes. Ainsi, depuis les attentats du 11 septembre 2001 à New York, la plupart des pays ont durci leur législation pénale après notamment le constat du recours aux nouvelles technologies par les membres de groupes terroristes. Ils ont renforcé en particulier les moyens d'investigation mis à la disposition des services d'enquête.

ASPECTS JURIDIQUES DE LA CYBERCRIMINALITÉ

Compte tenu du caractère mondial, planétaire d'*Internet* et des réseaux numériques, il convient d'aborder les principales évolutions législatives tant sur le plan national qu'international, avec en particulier la convention du Conseil de l'Europe sur la cybercriminalité, premier traité international en ce domaine.

L'arsenal juridique français

Le droit pénal français, par la loi n° 78-17 du 6 janvier 1978 modifiée dite « loi informatique et libertés » a dans un premier temps perçu l'ordinateur comme susceptible de porter atteintes aux droits de la personne, mais nullement comme un instrument criminogène. Progressivement, le législateur a abordé ce phénomène en le qualifiant initialement de « criminalité informatique »⁽⁶⁾ ce qui permet d'appréhender plusieurs infractions commises en lien avec l'ordinateur, la notion de cybercriminalité étant plus récente.

(6) Expression qui correspond en droit anglo-saxon à la notion de « *computer crime* ».

Cybercriminalité : aspects
stratégiques et juridiques

Grâce à la loi n° 88-19 du 5 janvier 1988 dite « loi Godfrain », la France s'est dotée d'un dispositif répressif destiné à la lutte contre les manifestations du crime informatique visant à assurer la sécurité des systèmes d'information et à réprimer la fraude informatique. Les délits informatiques se trouvent désormais codifiés dans les articles 323-1 et suivants du code pénal, dans la section « des délits contre les systèmes de traitement automatisé de données ». Ils constituent le noyau dur de la criminalité informatique telle qu'elle était appréhendée initialement.

Ces dispositions répriment l'accès frauduleux dans un système informatique, et visent toute pénétration matérielle dans tout ou partie du système, comme par exemple l'intrusion par obtention des codes d'accès de façon irrégulière, les manipulations illicites, l'emploi d'un cheval de Troie. L'absence d'autorisation légale, administrative ou contractuelle pour accéder aux données est la seconde condition pour que l'infraction soit caractérisée. La loi n'a pas cependant précisé si l'accès illégal impliquait ou non la violation des dispositifs de sécurité. La seconde infraction est le maintien non autorisé dans un système, prévue par l'article 323-1 du code pénal et présente un intérêt particulier par rapport à l'infraction précédente. Il s'agit par exemple de la personne qui a accédé régulièrement, mais qui s'est maintenue dans le système alors qu'elle n'était pas autorisée à le faire. Tel est le cas de la personne qui a accédé régulièrement à un service informatique et qui s'y maintient en envoyant des messages destinés à corrompre des clients.

Enfin, l'entrave volontaire au fonctionnement du système prévue par l'article 323-2 du code pénal est un délit spécifique même s'il intervient postérieurement à des faits d'accès frauduleux. Les moyens utilisés pour porter atteinte aux systèmes sont multiples. Il peut s'agir de la destruction de matériel, de virus, de bombes logiques, de changement de code, d'envois massifs de messages dit *melbombing* ⁽⁷⁾. L'entrave peut être périodique ou permanente par perturbation du système. L'élément fondamental de l'infraction est constitué par l'action frauduleuse délibérée qui empêche un fonctionnement normal du système.

(7) Tribunal de grande instance de Nanterre, 15^e chambre, 8 juin 2006, site forum des droits de l'Internet (www.foruminternet.org).

Cybercriminalité : aspects
stratégiques et juridiques

La loi réprime enfin la participation à un groupe de personnes en vue de préparer une ou plusieurs infractions informatiques évoquées ci-dessus transposant ainsi l'infraction d'association de malfaiteurs au monde des réseaux numériques. Cette incrimination est souvent retenue pour sanctionner des actes de complicité plutôt que pour réprimer les actes préparatoires au délit. Afin d'établir l'infraction, il convient de rassembler des éléments objectifs, comme l'échange de matériels, de codes d'accès, de logiciels ce qui est parfois complexe en pratique. La tentative de ces infractions est punissable à l'exception du délit d'entente ⁽⁸⁾ et les personnes morales peuvent être déclarées responsables (article 323-6 du CP).

Les articles 323-1 et suivants du code pénal répriment, au chapitre des atteintes aux systèmes de traitement automatisé des données, le fait d'accéder ou de se maintenir dans un système de traitement automatisé, ou d'en modifier le contenu, d'en entraver le fonctionnement ou d'y introduire des données, ou d'en modifier le fonctionnement. L'association de malfaiteurs, définie comme la participation à un groupement formé ou à une entente établie, en vue de la préparation, caractérisée par un ou plusieurs faits matériels d'une ou plusieurs infractions, est spécialement incriminée lorsqu'elle est constituée en vue de commettre des atteintes aux systèmes de traitement automatisé des données.

**La loi n° 2001-1062 du 15 novembre 2001
relative à la sécurité quotidienne**

Force est de constater que l'émergence d'actions et d'attentats terroristes a accéléré les évolutions législatives concernant les réseaux numériques et l'*Internet*. Ainsi, la loi du 15 novembre 2001 a posé le principe de la conservation pour une durée d'un an des données de connexion des abonnés par les opérateurs de téléphonie fixe et mobile et aux fournisseurs d'accès à *Internet* pour les besoins d'une procédure pénale ⁽⁹⁾.

Le texte pose un principe, celui de l'effacement des données, accompagné de trois exceptions autorisant la conservation des données de connexion, à savoir d'une part la recherche, la constatation et

(8) Article 323-7 du Code pénal.

(9) Article L. 34-1 du code des postes et des communications électroniques.

Cybercriminalité : aspects
stratégiques et juridiques

la poursuite des infractions pénales, pour les besoins de facturation des entreprises et pour des questions de sécurité informatique.

La loi permet aussi aux autorités judiciaires de disposer désormais de moyens renforcés de l'État couvert par le secret de la défense nationale aux fins de procéder à un décryptage des données. Tel est le cas lorsqu'un moyen de cryptologie aurait été utilisé pour commettre un crime ou un délit en matière de terrorisme par exemple.

Cette loi a créé un observatoire de la sécurité des cartes de paiement afin de cerner ce contentieux de masse que représente notamment la contrefaçon de cartes bancaires.

**La loi n° 2004-575 du 21 juin 2004 pour la confiance
dans l'économie numérique**

Ce texte fondateur met en place un statut juridique de l'*Internet* et vise à sécuriser son usage en clarifiant le régime de responsabilités des prestataires de service tout en mettant en œuvre une protection efficace pour les internautes.

Les prestataires techniques, aux termes de l'article 6 de la loi n'ont pas d'obligation générale de surveillance et de recherche d'activités illicites notamment en ce qui concerne les contenus qu'ils hébergent, transportent ou stockent. Ainsi, le statut « d'hébergeur » comporte un régime de responsabilité moins étendu au regard des contenus hébergés que celui « d'éditeur ».

En revanche, ils ont une obligation spéciale de concourir à la lutte contre l'apologie des crimes contre l'humanité, l'incitation à la haine, la pornographie infantine, l'incitation à la violence, les atteintes à la dignité humaine. À cette fin, ils doivent mettre en place un dispositif technique de dénonciation de ce type de données et informer promptement les autorités publiques compétentes de toutes activités illicites portées à leur connaissance. Ils doivent en outre rendre publics les moyens consacrés à la lutte contre ces activités. Le rapport de l'Assemblée nationale, publié récemment ⁽¹⁰⁾, préconise même d'élargir cette obligation de publicité aux atteintes aux intérêts privés, tels la diffamation, les droits d'auteur et la contrefaçon.

(10) Consultable sur le site www.juriscom.net.

Cybercriminalité : aspects
stratégiques et juridiques

Cette loi sécurise les échanges et amplifie les moyens de lutte contre la cybercriminalité en réprimant, par exemple, l'importation, la détention, l'offre, la cession ou la mise à disposition sans motif légitime d'éléments d'intrusion comme des virus.

Elle met aussi en place un cadre pour l'économie numérique comme la délimitation de l'e-commerce, la responsabilité des commerçants en ligne, l'encadrement juridique des instruments de commerce électronique. Enfin, elle améliore, tout en l'encadrant, l'accès des personnes privées aux moyens de cryptologie.

**La loi n° 2006-64 du 23 janvier 2006 relative
à la lutte contre le terrorisme**

Ce texte relatif à la lutte contre le terrorisme et portant dispositions diverses sur la sécurité et les contrôles frontaliers a pris en compte l'importance du réseau *Internet* comme vecteur d'échange d'informations à caractère terroriste.

La loi a complété la liste des personnes soumises à l'obligation de conservation et de communication à la justice des données techniques, tels les cybercafés et les bornes *Wifi* ⁽¹¹⁾ qui sont désormais assimilés à des opérateurs de communication électroniques. Cette disposition a ainsi pour objectif de permettre aux services de police d'identifier les clients d'un cybercafé et de cerner les connexions car il a été souvent constaté que les terroristes échangeaient avant de commettre des attentats.

Le décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques en a précisé la liste. Cependant, en pratique, les services de lutte contre le terrorisme déplorent l'absence d'obligation d'identification des clients ayant recours à ces services constitue une réelle limite à l'utilité de la disposition. Il serait à cet égard peut être pertinent de s'inspirer de la législation italienne qui exige la sollicitation d'une autorisation préalable ainsi que l'identification de l'ensemble des clients ⁽¹²⁾.

(11) L'article 5 de cette loi, portant création de l'article L 34-1-1 du code des postes et des télécommunications, permet l'assimilation des cybercafés à des opérateurs de téléphonie.

(12) Voir sur ce point le rapport de la commission des lois sur la mise en application de la loi n° 2006-64 du 23 janvier 2006 (www.legifrance.gouv.fr).

Cybercriminalité : aspects
stratégiques et juridiques

La loi a créé un dispositif d'accès de certains agents des services chargés de la prévention du terrorisme aux données conservées par les opérateurs de communication électroniques et les hébergeurs de site *Internet* ⁽¹³⁾.

**La loi n° 2006-961 du 1^{er} août 2006 relative
au droit d'auteur et aux droits voisins**

Transposition de la directive du 22 mai 2001, relative au droit d'auteur, ce texte vise à préserver les droits des créateurs. Sur le plan de la cyberdélinquance, trois axes sont à signaler.

En premier lieu, l'offre de moyens illicites de mise à disposition du public d'œuvres ou objets protégés, est réprimée. Les éditeurs et les distributeurs de logiciels dédiés ou utilisés dans ce but sont passibles du délit de contrefaçon.

Les logiciels d'échange de données ou de fichiers configurés spécifiquement pour faire circuler des fichiers contenant des mesures techniques de protection sont exclus de cette catégorie.

Les peines complémentaires sont la confiscation des recettes tirées de l'exploitation du logiciel litigieux, la publication du jugement, la fermeture de l'établissement ou encore l'interdiction d'exercer l'activité d'édition ou de distribution de logiciels.

En second lieu, la mise à disposition du public d'œuvres en violation des droits d'auteur constitue une forme illicite de représentation ou de communication au public punie par le délit de contrefaçon.

Le fait que cette mise à disposition illicite précède la mise à disposition officielle du public en France, violant ainsi le principe de « la chronologie des médias » issu de la loi n° 82-652 du 29 juillet 1982 ⁽¹⁴⁾ sur la communication audiovisuelle, est considéré comme une circonstance aggravante. Les internautes qui utilisent des logiciels *peer to peer* les obligeant à mettre à disposition des autres usagers les fichiers lors du téléchargement ⁽¹⁵⁾ sont exclus de cette catégorie.

(13) Disposition applicable suite à la parution du décret n° 2006-1651 du 22 décembre 2006 pris pour l'application du I de l'article 6 de la loi n° 2006-64 du 23 janvier 2006 qui précise que les demandes de réquisitions administratives doivent être faites par des agents habilités.

(14) Loi publiée au JO du 30 juillet 1982 (www.legifrance.gouv.fr).

(15) Ce qui est le cas, par exemple, du logiciel *emule*.

Enfin, les internautes effectuant des téléchargements illicites font l'objet par leurs fournisseurs d'accès à *Internet* (FAI) de mise en garde préalable et de messages de sensibilisation. Le téléchargement constituant une reproduction d'une œuvre en fraude des droits de son auteur, ce qui est constitutif d'un acte de contrefaçon, sanctionné pénalement. Des peines exclusivement pécuniaires sont prévues ici, toujours avec une gradation : par exemple sont pris en compte la récidive, le nombre ou le volume élevé des téléchargements illicites, l'antériorité du téléchargement à la diffusion commerciale officielle, la mise à disposition automatique durant le téléchargement.

La jurisprudence s'est prononcée à de nombreuses reprises concernant les utilisateurs de *peer to peer* poursuivis pour reproduction ou diffusion non autorisée de programme, vidéogramme ou phonogramme, contrefaçon par édition ou reproduction d'une œuvre de l'esprit au mépris des droits d'auteur. Dans ce cas, l'exception de copie privée est expressément écartée ce qui est logique car cette dernière ne vise qu'un usage privé alors que dans l'hypothèse du téléchargement illicite, il s'agit d'une copie faite pour autrui.

Un échelonnement de la sanction pénale est officialisé entre la personne qui aura conçu et diffusé un logiciel permettant des échanges illicites et dont il tirera un revenu conséquent, la personne qui mettra en ligne un volume très important de fichiers illégaux et la personne qui, très ponctuellement, téléchargera une toute petite quantité de ces fichiers.

Même si cette gradation avait déjà cours de façon informelle, cela permettra d'éviter l'insécurité juridique liée aux différentes méthodes de calcul de la sanction pécuniaire.

Les internautes ne doivent oublier qu'à côté des sanctions pénales, la peine la plus lourde se situe souvent au niveau de la condamnation civile. En effet, le montant des dommages et intérêts réclamés par les titulaires de droit peut atteindre parfois plusieurs centaines de milliers d'euros.

Enfin, il convient de souligner qu'en dépit de la promulgation de la loi n° 2006-961 du 1^{er} août 2006 relative au droit d'auteur et aux droits voisins, la réflexion afin de trouver des solutions au problème du téléchargement illicite, complémentaire de la répression de la contrefaçon n'est certainement pas en l'état aboutie.

En effet, les réponses pénales semblent quelque peu disproportionnées ; d'ailleurs les tribunaux n'ont jamais prononcé de peines d'emprisonnement ferme et les amendes sont généralement faibles et assorties du sursis.

Les lois du 5 mars 2007 relatives à la prévention de la délinquance et réformant la protection de l'enfance

Tenant compte de l'utilisation croissante par les jeunes des nouvelles technologies, en particulier d'*Internet*, la loi relative à la prévention de la délinquance vise à améliorer leur protection contre des utilisations délictueuses. Par exemple, cette loi a prévu la signalisation de l'interdiction aux mineurs des supports vidéo à contenu violent, emportant l'interdiction de louer, de proposer ou de vendre ceux-ci à des mineurs.

Par ailleurs, l'utilisation d'un moyen de communication électronique pour faire une proposition sexuelle à un mineur constitue une infraction spécifique, la peine étant majorée lorsque cet agissement est suivi d'une rencontre. Sans sombrer dans l'inventaire, il faut comprendre que la norme pénale s'adapte constamment aux évolutions non seulement techniques mais comportementales. Ainsi, la loi a créé un nouveau délit, le *happy slapping* qui réprime les actes d'enregistrement et de diffusion d'images d'agressions afin de répondre à l'essor de ce nouveau phénomène de violence gratuite.

Dans le domaine du renforcement des moyens d'investigation ce texte donne l'autorisation aux policiers et aux gendarmes d'infiltrer les réseaux numériques tels *Internet* pour repérer les délinquants et les interpellier lors d'enquêtes dans le domaine de la corruption de mineurs et de la pédopornographie, mais aussi en matière de traite des êtres humains, du recours à la prostitution de mineurs et de proxénétisme.

Dans ce cadre, sous réserve que leurs actes ne constituent pas une incitation à commettre les infractions, les policiers et gendarmes peuvent devenir des « cyber-patrouilles » c'est-à-dire qu'ils peuvent participer aux échanges électroniques sous un pseudonyme et entrer en contact avec les auteurs d'infractions.

Cybercriminalité : aspects stratégiques et juridiques

Enfin, la loi portant réforme de la protection de l'enfance crée un article 227-23, alinéa 5 du Code pénal qui réprime la consultation habituelle d'images pédopornographiques.

La France poursuit son action en la matière et un plan d'action a été lancé dernièrement par le gouvernement qui constitue une nouvelle étape de la lutte contre la cybercriminalité. Une charte de bonnes pratiques avec les opérateurs de communications électroniques va être élaborée. Par ailleurs de nouvelles incriminations sont prévues dans le cadre de la prochaine loi d'orientation et de programmation pour la sécurité intérieure (Lopsi), comme l'usurpation d'identité par *Internet*.

L'arsenal international en matière de cybercriminalité

Internet est un réseau de communication ouvert qui permet la diffusion de tous types d'informations en niant toute contrainte géographique. Suivant la loi applicable dans le pays de destination de l'information, cette dernière peut être considérée comme illicite ou licite suivant la conception qu'on les États de la liberté d'expression et de la protection de la vie privée. Des instruments juridiques internationaux, à savoir la Convention et son protocole additionnel du conseil de l'Europe sont venus utilement apporter des définitions communes des infractions et proposer des instruments d'investigation tout en préconisant le développement de la coopération internationale indispensable à l'efficacité de la lutte contre ce phénomène multiforme.

La convention du Conseil de l'Europe

La Convention sur la cybercriminalité du Conseil de l'Europe, ouverte à la signature en 2001 est entrée en vigueur en 2004. Seul instrument international contraignant en ce domaine, elle définit des lignes directrices pour tout pays élaborant une législation exhaustive en matière de cybercriminalité, et sert de cadre pour la coopération internationale, car conçue pour avoir une portée mondiale. Ainsi le Canada, le Japon, l'Afrique du Sud et les États-Unis ont participé à son élaboration, l'ont signée avant de la ratifier (2006). La Convention est complétée par un protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (que n'ont pas signé les États-Unis). En qualifiant d'infractions pénales certains agissements et non la technologie en elle-même,

Cybercriminalité : aspects
stratégiques et juridiques

la Convention a su rester d'actualité et est tout à fait pertinente face à des phénomènes tels que le *phishing* et les autres formes d'usurpation d'identité, le déni de service ou le cyberterrorisme. La Convention est ouverte à l'adhésion de tout pays qui le souhaite. En février 2008, elle était déjà ratifiée par 22 pays et signée par 21 autres.

Des travaux sont actuellement en cours, dans le cadre du projet du Conseil de l'Europe sur la cybercriminalité, afin d'élaborer des lignes directrices pour aider les fournisseurs d'accès et les services répressifs à structurer leur coopération tout en évitant les violations de la vie privée. Le Conseil de l'Europe assure un suivi et un appui dans la mise en œuvre de la convention et organise des rencontres internationales.

En conclusion, il apparaît que la France dispose d'un arsenal juridique permettant une lutte efficace contre la cybercriminalité, ainsi que des services spécialisés de défense nationale et de sécurité du territoire. Dans le cadre de la prochaine présidence française du Conseil de l'Union européenne, des accords internationaux permettant la perquisition informatique à distance sans demande d'autorisation préalable du pays hôte du serveur seront étudiés. Il convient de créer désormais une « véritable toile », un maillage entre les services d'enquête et l'institution judiciaire, et de renforcer la coopération internationale entre l'ensemble des pays concernés afin d'éviter la création de « cyberparadis ».

Myriam QUÉMÉNER

Myriam Quéméner, Magistrat, est Substitut général à la Cour d'Appel de Versailles. Elle est l'auteur avec Joël Ferry de *Cybercriminalité : défi mondial et réponses* (Economica, 2008).