

Citation : Eric A. Caprioli, *Les moyens juridiques de lutte contre la cybercriminalité*, www.caprioli-avocats.com

Première publication : **Revue Risques n°51, Les cahiers de l'assurance**, Ed. LGDJ/SEDDITA, juillet-sept 2002, p. 50-55.

Date de la mise à jour : juillet 2002

LES MOYENS JURIDIQUES DE LUTTE CONTRE LA CYBERCRIMINALITE

Par [Eric A. Caprioli](#)

contact@caprioli-avocats.com

PLAN

[Introduction](#)

[La conservation des données de connexion](#)

[L'accès aux contenus des messages : Interceptions de sécurité et déchiffrement des données codées](#)

[1. L'harmonisation des infractions](#)

[2. Falsifications et fraudes informatiques](#)

[3. Pornographie enfantine](#)

[4. Les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes](#)

[La responsabilité pénale des personnes morales](#)

[Les procédures et perquisitions](#)

[Notes](#)

Introduction

Les réseaux numériques sont devenus une composante majeure sur laquelle repose la croissance de nos économies. Pourtant, l'utilisation des réseaux tels l'internet présentent des risques et des vulnérabilités inhérentes à leur nature ouverte et internationale. 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 TIC (Technologies de l'Information et de la Communication). Chacun a en mémoire la récente affaire Yahoo! (Ordonnance de Référé du 20 novembre 2000, TGI Paris), qui a ouvert une brèche dans le principe de territorialité du droit pénal. En effet, le juge des référés français, a condamné une entreprise américaine, sur le fondement du droit français (article R-645-1 du code pénal), pour des faits (ventes d'objets nazis) commis virtuellement sur le territoire français, à partir du territoire américain.

Pour autant, les activités criminelles liées aux technologies de l'information ne se limitent pas à des actes racistes ou néo-nazis ; en effet, elles peuvent prendre des formes très variées : atteintes aux systèmes d'information et/ou aux données informatisées, attaques de serveur par saturation (spamming), violation du secret des correspondances privées, violation des règles de protection des données personnelles, espionnage industriel ou militaire, contrefaçon de droits de propriété intellectuelle (brevets, marques, dessins, droits d'auteur, ...), délits de presse (ex : diffamation), fraude fiscale, fraude à la carte bancaire, blanchiment d'argent, réseaux de pédophiles, usurpation d'identité, organisation de la prostitution, ... La liste des infractions est longue ; ces dernières touchent aussi bien l'entreprise et les administrations que les individus. Par ailleurs, la diffusion de certains virus (ex : Melissa, Iloveyou, Code Red) ([1](#)) a causé d'importants dommages aux entreprises et autres organismes publics. Leurs modes de propagation sont divers : e-mail, Web, partage de réseau, etc. Plus récemment, des activistes se sont livrés à des activités de terrorisme sur les réseaux. A la suite des attentats du 11 septembre 2001, il a été annoncé que les terroristes d'Al-Qaïda avaient eu recours aux systèmes de messageries électroniques associés à l'usage de moyens de cryptologie et de stéganographie pour assurer la confidentialité de leurs échanges tendant à la préparation et à l'organisation de leurs attentats.

En tant qu'espace de communication ouvert, l'internet permet la diffusion de tout type d'information sans aucune contrainte géographique. Suivant la loi applicable dans le pays de destination de l'information, cette dernière pourra être considérée comme licite ou illicite, parfois en fonction des principes (variables) de liberté d'expression et de respect de la vie privée.

En matière de criminalité informatique ou de criminalité informatisée (que l'on nomme ensemble usuellement "cybercriminalité"), dès lors que le recours à l'appareil répressif est décidé par la victime ou par le Ministère Public, une réalité classique s'impose : le droit pénal est une des expressions de la souveraineté des États, en fonction de laquelle il possède une dimension territoriale. Or, l'internet s'affranchit de toute contrainte territoriale. En effet, en matière pénale, le juge d'instruction et la police judiciaire recherchent classiquement et principalement à localiser et identifier l'auteur d'une infraction et à préserver les éléments de preuve pour matérialiser l'infraction qui peuvent se trouver sur le territoire d'un autre État.

Le fait d'appréhender des comportements délictueux sur les réseaux se heurte à trois types de contraintes :

- * l'anonymat qui peut être organisé sur les réseaux. L'utilisation des services des prestataires de services de certification, tels que la société Certinomis ([2](#)), qui fournissent des certificats électroniques d'identification et de confidentialité, peut jouer un rôle non négligeable en terme de sécurité, et ce d'autant que des obligations légales s'imposent à eux tant pour le recouvrement des clés de chiffrement que pour la lutte contre l'anonymat ;
- * la volatilité des informations numériques (possibilité de modifier et de supprimer des éléments de preuve quasi instantanément) ;

* les comportements délictueux qui revêtent souvent un caractère transnational.

Face à ces réalités, une harmonisation internationale du droit et des procédures ainsi qu'une étroite coopération judiciaire sont des conditions sine qua non pour être en mesure de lutter efficacement contre des cybercriminels qui tendent à s'organiser et à agir au niveau planétaire. Cette harmonisation est devenue une priorité majeure des États qui sont entrés dans la société de l'information, spécialement les États membres du Conseil de l'Europe, conformément aux bases qui ont été définies par le G8. C'est dans cette perspective que la Convention du Conseil de l'Europe sur la cybercriminalité a été signée le 23 novembre 2001 à Budapest par 33 États, dont les membres de l'Union européenne, les États-Unis d'Amérique, le Canada, le Japon et l'Afrique du Sud ([3]). Cette Convention présente l'avantage d'énoncer les mesures que les États doivent adopter, mais sans que leur contenu soit précisé. Ceci explique pourquoi, concernant l'harmonisation des sanctions relatives aux attaques visant les systèmes d'information, la Commission européenne vient de publier une proposition de décision cadre le 19 avril 2002 ([4]).

Lors de la réunion du G8 des 13-14 mai 2002 au Canada, de nouvelles recommandations ont été adoptées sur les crimes de hautes technologies, les crimes informatiques et les moyens de lutte y associés ([5]).

Les enjeux juridiques sont à la mesure des pertes financières et des dommages résultant de la cybercriminalité qui ont connu une forte progression, encore accrue, au cours de ces dernières années. Ainsi, du point de vue de l'assurance, si les risques matériels et immatériels (données numérisées) sont assurables en vertu de leur caractère aléatoire, il en va différemment des risques pénaux nés de la commission des infractions relatives à la cybercriminalité. Il n'en demeure pas moins que l'analyse des moyens juridiques de lutte contre la cybercriminalité permet de mettre en relief le contenu de l'arsenal répressif existant.

Envisageons tour à tour les principaux aspects de la lutte contre la cybercriminalité.

La conservation des données de connexion

En vertu de la Convention du Conseil de l'Europe, les États ont l'obligation d'adopter les mesures nécessaires afin de pouvoir enjoindre à une personne ou à une entreprise de conserver certaines données informatiques stockées ou des données de connexion relatives à une infraction pénale, sous le sceau du secret procédural, notamment lorsque ces données risquent de disparaître ou d'être modifiées et de pouvoir les divulguer à l'autorité compétente de l'État partie. De la même manière, les États doivent habiliter leurs autorités compétentes à avoir le pouvoir d'enjoindre aux personnes présentes sur leur territoire et aux fournisseurs de services internet à communiquer les informations en leur possession.

La France est intervenue en ce domaine avec la loi du 1^{er} Août 2000 (réformant la loi du 30 septembre 1986 sur la liberté de communication) qui encadre la responsabilité et les obligations des fournisseurs d'accès à l'internet (F.A.I.) et des fournisseurs d'hébergement. Elle leur impose d'identifier leurs clients bénéficiant de services d'accès à l'Internet et leur donne obligation de conserver et de communiquer ces données identifiantes sur réquisition de l'autorité judiciaire. Toutefois elle ne précisait pas combien de temps les F.A.I. avaient l'obligation de conserver ces données, ni ce qu'il convient d'entendre par autorité judiciaire (les demandes d'un O.P.J. semblent *a priori* exclues). Par ailleurs, les personnes physiques ou morales dont l'activité est d'éditer un service de communication en ligne, autre que des correspondances privées, doivent s'identifier précisément et tenir ces informations à la disposition du public.

De plus, la loi sur la sécurité quotidienne (L.S.Q.) du 15 novembre 2000 ([6]) impose aux opérateurs de télécommunications la conservation des données de connexion des internautes pendant une durée de un an avec pour finalité de mettre à la disposition des autorités judiciaires des informations nécessaires à l'enquête ([7]). Cependant, les modalités de conservation doivent encore être précisées par décret. Ces dispositions législatives figurent dans un Chapitre intitulé : « *Dispositions renforçant la lutte contre le terrorisme* ». L'article 22 de la loi trace la perspective dans laquelle s'inscrivent les dispositions légales : « *Afin de disposer des moyens impérieusement nécessaires à la lutte contre le terrorisme alimenté notamment par le trafic de stupéfiants et les trafics d'armes et qui peut s'appuyer sur l'utilisation des nouvelles technologies de l'information et de la communication, les dispositions du présent chapitre sont adoptées pour une durée allant jusqu'au 31 décembre 2003. Le Parlement sera saisi par le Gouvernement, avant cette date, d'un rapport d'évaluation sur l'application de l'ensemble de ces mesures.* ». Il convient de préciser, en outre, que la loi de finance rectificative pour 2001 du 28 décembre 2001 a élargi l'accès aux données de connexion auprès des fournisseurs d'accès et des opérateurs de télécommunications, alors que la L.S.Q. réservait cette possibilité aux seuls juges, aux agents des douanes, du fisc et aux enquêteurs de la Commission des Opérations de Bourse (C.O.B.) ([8]).

La conservation de ces données a pour objectif de permettre l'identification des délinquants et de matérialiser des éléments de preuve des infractions. Néanmoins, ces mesures peuvent s'avérer insuffisantes si l'État en cause ne se dote pas des moyens juridiques appropriés pour procéder à des interceptions légales et aux déchiffrements des messages codés suspects.

L'accès aux contenus des messages : Interceptions de sécurité et déchiffrement des données codées

Les autorités compétentes des États parties à la Convention sur la cybercriminalité pourront collecter les données de connexion et intercepter les données relatives au contenu directement ou en contraignant les fournisseurs de services internet (ex : le système Carnivor du F.B.I. aux U.S.A.). Le libellé de la Convention permettra à chaque pays d'adapter un système d'interception à sa législation interne. Pour ce qui est de la France, l'autorité judiciaire a déjà la possibilité de procéder par voie de réquisition auprès des opérateurs téléphoniques qui ont l'obligation de fournir les données de connexion (la prestation est facturée environ 90 €). En ce qui concerne le contenu des communications, c'est le régime classique sur les

écoutes téléphoniques (procédure judiciaire) et les interceptions de sécurité (procédure administrative) qui a vocation à s'appliquer, sans qu'il y ait besoin de profonde modification (loi du 10 juillet 1991). C'est en ce sens que la L.S.Q. a anticipé l'adoption de la Convention. Un nouvel article 11-1 a été introduit dans la loi du 10 juillet 1991, aux termes duquel les autorités judiciaires pourront avoir accès aux conventions de chiffrement des données chiffrées du présumé délinquant par l'entremise des prestataires de services de cryptologie ([9]).

En outre, d'une part, la L.S.Q. introduit plusieurs articles dans le code de procédure pénale afin de permettre aux magistrats (du parquet, de l'instruction et de la juridiction de jugement) d'ordonner le déchiffrement des données. D'autre part, elle établit une nouvelle incrimination avec l'introduction de l'article 434-15-2 dans le code pénal : toute personne qui a connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, a l'obligation de remettre ladite convention aux autorités ou de la mettre en œuvre. En cas de défaut d'exécution, des peines de prisons et d'amende sont prévues ([10]). Ces nouvelles dispositions doivent interpeller les assureurs auxquels s'imposera l'obligation de limiter leur garantie à certains coûts liés à la reconstitution des clés de chiffrement des clients des prestataires qu'ils assurent.

1. L'harmonisation des infractions

Les États parties à la Convention s'engagent à adopter en conformité avec leur droit interne des législations qui définissent un certain nombre d'infractions ainsi que leur tentative de commission, tout en laissant aux États une marge d'adaptation plus ou moins large selon les faits visés. En droit français, ces incriminations reprennent globalement la substance de la loi Godfrain du 5 janvier 1988 (articles 323-1 à 323-7 du code pénal). Les États doivent prendre les mesures nécessaires pour que les infractions visées soient sanctionnées par des " *sanctions effectives, proportionnées et dissuasives y compris la privation de liberté*". Ils doivent adopter des législations incriminant les infractions suivantes :

Infractions contre la confidentialité, l'intégrité et la disponibilité des données et des systèmes informatiques.

Sont ainsi incriminés l'accès illégal, les interceptions illégales, l'atteinte à l'intégrité des données, l'atteinte à l'intégrité du système et les abus de dispositifs informatiques permettant la commission d'infractions.

2. Falsifications et fraudes informatiques

Sont ici visées les modifications, altérations de données informatiques lorsqu'elles sont utilisées aux fins de paraître légales ou authentiques, ainsi que toute atteinte au fonctionnement d'un système informatique dans l'intention d'obtenir sans droit un bénéfice économique quelconque.

3. Pornographie enfantine

Sont incriminées toutes les productions, mises à disposition, diffusions, ou détention d'images de pornographie enfantine concernant des mineurs de 18 ans, voire de 16 ans en fonction du droit interne de chaque État ([11]). Cette disposition, particulièrement attendue par le grand public, revêt un caractère plus symbolique, qu'une nécessité purement juridique. En effet, rares sont les États qui n'ont pas légiféré ou qui n'ont pas de règles de prohibition en matière de protection des mineurs. A la vérité, la difficulté tient davantage à la non application par certains États de leur propre législation pour des raisons de corruption ou de politique pénale laissant apparaître, de fait, une certaine permissivité ou tout au moins une inertie judiciaire. C'est en réalité la différence entre les seuils de la majorité qui risque de poser des difficultés, notamment pour les pays qui opèrent une distinction entre la majorité civile et la majorité sexuelle.

4. Les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

Les atteintes aux droits protégés en vertu notamment des droits nationaux ou du Traité de l'OMPI sur le droit d'auteur (entrée en vigueur le 6 mars 2002) ou de la Convention de Berne (1886) doivent être réprimées. Le texte de la Convention prévoit ainsi un durcissement de la protection des droits de propriété intellectuelle par le fait que les atteintes seront systématiquement sanctionnées sur le plan pénal. Du point de vue français, cela ne bouleversera pas l'ordre juridique puisque l'actuelle victime d'une atteinte à un droit de propriété intellectuelle (contrefaçon) a le choix entre la voie civile à vocation purement indemnitaire, et la voie pénale à vocation répressive et indemnitaire par constitution de partie civile. En revanche, pour ce qui est des droits voisins (droits connexes dans la Convention), il faudra procéder à des ajustements législatifs. Pour d'autres pays, il s'agira de modifier substantiellement l'état actuel de leur droit.

La responsabilité pénale des personnes morales

Cette responsabilité peut être pénale, civile ou administrative lorsque les faits définis dans la Convention ont été commis par une personne physique ayant le pouvoir d'engager ou de représenter la personne morale ou lorsqu'elle exerce sur elle un contrôle. Elle doit être établie indépendamment de la responsabilité pénale des personnes physiques ayant commis les faits. En droit français, il est possible d'engager la responsabilité pénale d'une personne morale, sous la condition que le législateur l'ait prévu.

Les procédures et perquisitions

Les Etats parties à la Convention ont l'obligation d'habiliter leurs administrations respectives à perquisitionner les systèmes informatiques, à saisir des données et à imposer aux personnes concernées de fournir les données en leur possession, de conserver les données « vulnérables » ou de les faire conserver par les personnes concernées.

Les mesures prévues par la Convention sont applicables en droit interne à toutes les enquêtes et procédures pénales relatives aux infractions définies dans la Convention ainsi qu'à toute infraction commises au moyen d'un système informatique ou pour la collecte de preuves électroniques concernant une infraction pénale quelconque. Cette précaution vise à permettre une souplesse procédurale afin de rendre applicable la coopération procédurale lorsque l'enquête nécessite des investigations sur des moyens informatiques. La mise en œuvre des procédures doit être proportionnée avec la nature des circonstances de l'infraction et s'inscrire dans la conformité de l'ordre juridique interne et respecter les libertés fondamentales et les droits de l'homme.

Les autorités compétentes d'un Etat doivent pouvoir perquisitionner et saisir les informations relatives à une infraction liée à l'utilisation de l'informatique. La question des perquisitions à distance et transfrontalières dans des systèmes informatiques implantés dans un Etat partie, à partir d'un autre Etat a été abordée, mais aucune position commune n'a pu être adoptée, ni aucune mesure technique envisagée concrètement. Cette position était défendue par les Etats-Unis qui préféreraient voir en lieu et place du système de coopération judiciaire et d'entraide, instaurer une véritable « cyberpolice » internationale qui se jouerait des frontières. A cette omission volontaire, plusieurs raisons : la souveraineté des Etats est directement atteinte par de telles pratiques, et la plupart des Etats demeurent réticents à dévoiler qu'ils disposent déjà d'un arsenal technologique leur permettant d'opérer ce type de « visites » dans des systèmes d'information étrangers sans laisser de traces ...

En ce qui concerne la France, les dispositions pénales permettent déjà de saisir tout type d'information dans le cadre d'une enquête judiciaire. Néanmoins, le législateur prévoit dans le projet de loi sur la société de l'information (LSI) de modifier les articles 56 et 97 du code de procédure pénale en complétant le concept de « documents » par celui de « données informatiques » et le concept de « pièces » par celui d'« informations » et en organisant la saisie ou la copie des données informatiques.

En conclusion, nous observerons que pour mettre en œuvre cet arsenal pénal international, la Convention pose un principe général de coopération. La Convention du Conseil de l'Europe prévoit que les traités et accords internationaux de coopération en matière pénale, seront applicables aux infractions et procédures définies dans le corps du texte de la Convention. Il est certain que les Etats qui n'ont pas de retard technologique, ou qui chercheront à utiliser la Convention à des fins de politique interne, mettront les moyens matériels et humains en place. Mais d'autres pays, même s'ils sont partie à la Convention, - a fortiori s'ils ne le sont pas - demeureront, faute de moyens suffisants, de parfaits paradis informationnels que ne manqueront pas d'utiliser les professionnels du crime organisé sur les réseaux, tout en ayant acquis une respectabilité d'apparence en matière de lutte contre la cybercriminalité. Dans la mesure où les risques sont identifiés et que les paradis existent en droit français notamment, il reste à les prendre en considération dans la pratique de l'assurance des ressources informatiques et des réseaux.

Notes :

[1] Les virus informatiques se répartissent en plusieurs catégories : virus (résident ou non résident), vers, chevaux de Troie, bombes logiques. Les trois « virus » informatiques mentionnés ci-dessus sont des vers.

[2] V. <http://www.certinomis.com>. Cette société française est une filiale du groupe La Poste.

[3] Le texte est consultable sur le site <http://conventions.coe.int>.

[4] Proposition de décision cadre du Conseil relative aux attaques visant les systèmes d'information, COM (2002) 173 final du 19 avril 2002.

[5] Consultable sur le site : <http://q8-j.ca>.

[6] L. n°2001-1062, J.O. du 16 novembre 2001.

[7] Article 29 de la L.S.O., modifiant l'article L. 32-3 du Code des Postes et télécommunications

[8] Cela figure à l'article 62 de la LFR n°2001-1276, adoptée le 28 décembre 2001, J.O. du 29 décembre 2001, p.21133 ; article 65 du code des douanes ; article L. 83 du Livre des Procédures Fiscales ; article L. 621-10 Code monétaire et financier.

[9] En cas de non remise ou de non mise en œuvre des conventions secrètes, les personnes sont passibles de deux ans d'emprisonnement et de 30.000 € d'amende.

[10] Article 434-15-2, al. 1 : 3 ans d'emprisonnement et 45.000 € d'amende et Article 434-15-2, al. 2 : 5 ans d'emprisonnement et 75.000 € d'amende.

[11] V. l'article 13 de la Loi n°98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs, J.O. n°139, 18 juin 1998, p.9255, spécialement quant à la diffusion de messages pédophiles et quant à la mise en contact de mineurs avec l'auteur des faits grâce à l'utilisation d'un réseau de télécommunications (v. notamment les articles 225-7 et 227-22 code pénal).