**Cybercriminalité**

**Définition**

La cybercriminalité est une notion large qui regroupe « toutes les infractions pénales susceptibles de se commettre sur ou au moyen d’un système informatique généralement connecté à un réseau. »

Il s’agit donc d’une nouvelle forme de criminalité et de délinquance qui se distingue des formes traditionnelles en ce qu’elle se situe dans un espace virtuel, le « cyberespace ». Depuis quelques années la démocratisation de l’accès à l’informatique et la globalisation des réseaux ont été des facteurs de développement du **cybercrime**.

On peut alors aujourd’hui regrouper la cybercriminalité en trois types d’infractions :

* Les infractions spécifiques aux technologies de l’information et de la communication : parmi ces infractions, on recense les atteintes aux systèmes de traitement automatisé de données, les traitements non autorisés de données personnelles (comme la cession illicite des informations personnelles), les infractions aux cartes bancaires, les chiffrements non autorisés ou non déclarés ou encore les interceptions.
* Les infractions liées aux technologies de l’information et de la communication : cette catégorie regroupe la pédopornographie, l’incitation au terrorisme et à la haine raciale sur internet, les atteintes aux personnes, les atteintes aux biens.
* Les infractions facilitées par les technologies de l’information et de la communication, que sont les escroqueries en ligne, le blanchiment d'argent, la contrefaçon ou toute autre violation de propriété intellectuelle.

****

Scène de cybercrime

**Dispositif législatif et conventionnel de lutte**

**Le dispositif législatif et réglementaire français**

En France la cybercriminalité est prise juridiquement en compte depuis la loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978.

La Loi Godfrain du 5 février 1988 relative à la fraude informatique a introduit les articles 323-1 et suivants dans le Code pénal, concernant notamment la suppression ou modification de données (art 323-1 al 1), ou encore la tentative d’infraction sur un STAD (323-7).

La loi du 15 novembre 2001 relative à la sécurité quotidienne

La loi du 18 mars 2003 pour la sécurité intérieure

La loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité

La loi pour la confiance dans l'économie numérique du 21 juin 2004, qui a modifié les articles 323-1 et suivant du Code pénal. Cette loi a, en outre, modifié l’article 94 du Code de procédure pénale relatif à l’inclusion des données informatiques dans la liste des pièces susceptibles d'être saisies lors des perquisitions réalisées en flagrant délit ou au cours d'une instruction. (Ces perquisitions sont aussi régies par les art. 56 et 97 du Code de procédure pénale).

La loi du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle.

La loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

La loi du 5 mars 2007 relative à la prévention de la délinquance

Par ailleurs de nombreux textes réglementaires ont été adoptés. On peut citer pour exemple le décret du 24 mars 2006 sur la conservation des données de trafic prévu par la loi relative à la sécurité quotidienne.

La lutte contre la cybercriminalité est en pleine évolution et elle fait l’objet de nombreuses réflexions en France. Par exemple le plan de lutte contre la cybercriminalité qui a été présenté en février 2008 contient des mesures visant à moderniser les méthodes d’investigation. Par ailleurs, la même année, au mois d’octobre a été présenté le plan du numérique 2012 qui contient des propositions relatives à la lutte contre le cybercrime.

Malgré cette évolution permanente le dispositif législatif français en matière de cybercriminalité est « éparpillé » dans divers textes. 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 cybercriminel par le droit français. Myriam Quéméner et Joël Ferry, dans *Cybercriminalité Défi Mondial* (2ème édition) décrivent le dispositif législatif et réglementaire français comme un «  ‘maquis’ quelque peu ésotérique ».



Formation des enquêteurs à la cybercriminalité

**La convention sur la cybercriminalité du 23 novembre 2001**

Le 23 novembre 2001 les pays membres du Conseil de l’Europe ainsi que les États-Unis, le Canada, le Japon et l’Afrique du Sud, ont adopté la convention sur la cybercriminalité, aboutissement d'un long processus de négociations (vingt-sept versions antérieures et quatre années de négociations officielles). Il s’agit d’une convention pénale à vocation internationale destinée à lutter contre le cybercrime. En 2007, seuls 14 États avaient ratifié la convention sur les 47 signataires.

Par ailleurs en 2003, a été ouvert à la signature le protocole additionnel à la convention sur la cybercriminalité, qui visait à élargir le champ d’application de la convention aux infractions de propagande raciste ou xénophobe commis via les réseaux internet. Ce protocole, non ratifié par les États-Unis, prévoit par ailleurs des mesures facilitant l’extradition et l’entraide judiciaire.

La France a ratifié ces deux textes par la loi n° 2005-493 du 19 mai 2005 autorisant l'approbation de la Convention du Conseil de l'Europe sur la cybercriminalité et du protocole additionnel à cette Convention1.

La convention sur la cybercriminalité de 2001 poursuit trois objectifs déterminés :

* L’harmonisation des législations des États signataires
* La modernisation de ces législations, notamment en matière procédurale
* L’amélioration de la coopération internationale en matière d’extradition et d’entraide répressive.

Le premier axe est l’harmonisation des législations nationales en ce qui concerne la définition des infractions répertoriées par la Convention. Il s'agit donc d'incriminer quatre séries d'infractions qui sont :

I. Les infractions informatiques : falsification et fraude informatique.

II. Les infractions de contenu : la pornographie enfantine. Le protocole additionnel inclut la propagation via Internet d’idées racistes et xénophobes.

III. Les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes : le partage non autorisé via Internet des œuvres protégées.

IV. Les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes : accès illégal, interception illégale, atteinte à l'intégrité des données ou des systèmes.

Ensuite, le deuxième axe, d'ordre procédural, définit les moyens d'enquêtes et de poursuites pénales les mieux adaptés à la mondialisation du réseau Internet. La Convention prévoit des règles pour garantir les droits des individus, mais aussi pour faciliter la conduite d'enquête. En ce sens, on peut citer, entre autres, les règles régissant la conservation des données stockées, la conservation et la divulgation rapide des données relatives au trafic, la perquisition des systèmes informatiques, la saisie de données informatiques, la collecte en temps réel des données relatives au trafic et l'interception de données relatives au contenu.

Enfin, le troisième axe concerne la mise en place d'un système rapide et efficace de coopération internationale. À côté des formes traditionnelles de coopération pénale internationale, prévues notamment par les Conventions européennes d'extradition et d'entraide judiciaire, la Convention sur la cybercriminalité prévoit des formes d'entraide correspondant aux pouvoirs définis préalablement par la Convention. Ces conditions sont exigées afin que les autorités judiciaires et les services de police d'un État membre puissent agir pour le compte d'un autre État dans la recherche de preuves électroniques, sans toutefois mener d’enquêtes ni de perquisitions transfrontalières. En outre, toute donnée obtenue devrait être rapidement communiqué à l'État intéressé.

Sans doute, ce texte international - constitue un complément indispensable aux lois nationales pour contenir le phénomène de cette nouvelle criminalité "caméléon" dont on ne connaît pas encore - du moins avec certitude - toutes "les couleurs" et les menaces2.

Par ailleurs, le 17 janvier 2005 le Conseil de l'Union européenne a adopté la décision cadre 2005/222/JAI du Conseil «  relative aux attaques visant les systèmes d’information », qui va permettre une harmonisation des règles pénales concernant les principales activités criminelles visant les systèmes d’information, l’atteinte à l’intégrité d’un système et l’atteinte à l’intégrité des données.

**Les acteurs**

**Les cyber délinquants ou cyber criminels et leurs victimes**

Historiquement, le cybercrime était le fait de particuliers souvent des étudiants, qui pénétraient un ou plusieurs réseaux, pour des mobiles divers.[réf. nécessaire]

Contrairement à ce que laisse suggérer les médias, 60 % des cyberattaques dans le monde en 2011 ne proviennent pas de Chine mais des États-Unis3.

**Les organes français de lutte**

La cybercriminalité est reconnue par beaucoup d’experts comme étant la nouvelle forme de criminalité du XXIe siècle. Dès lors pour la contrôler, la France a mis en place de nombreux organes de lutte. En voici, quelques exemples :

Dès 1998, a été créé, au sein de la gendarmerie, le département de lutte contre la cybercriminalité au sein du service technique de recherches judiciaires et de documentation (STRJD).



Logo du service technique de recherches judiciaires et de documentation

Le 15 mai 2000 a été créé l’Office central de lutte contre la criminalité liée aux technologies de l’information et de la communication (OCLCTIC), au sein de la direction centrale de la police judiciaire au Ministère de l’Intérieur. Elle regroupe notamment en son sein la plate-forme de signalement des contenus illicites sur internet. Cette même année, en complément de l’action de l’OCLCTIC, a été mise en place, la Direction de la surveillance du territoire, qui est compétente pour diligenter des enquêtes judiciaires relatives à des actes de piratage sur les systèmes informatiques des établissements à régime restrictif ou des données classifiées de défense.



Logo de la DST

Par ailleurs, en 2006 a été créé l’OCRVP, office central pour la répression des violences aux personnes, dont la mission est la coordination, sur le plan national, de la lutte contre les infractions violentes à l’encontre des personnes, notamment concernant la pédopornographie sur internet.

Enfin, la police nationale dispose de services spéciaux comme le SITT service de l’informatique et des traces technologiques. Les directions inter régionales et régionales de police judiciaire disposent d’ICC (Investigateurs en CyberCriminalité) anciennement dénommés ESCI (Enquêteurs Spécialisés en Criminalité Informatique). Il existe, en outre, différentes brigades spécialisées, telle la BEFTI brigade d’enquête sur les fraudes aux technologies de l’information.

**Les organes européens de lutte**

Les États ont rapidement compris que pour être plus efficace la lutte contre la cybercriminalité devait être européenne. Des compétences dans ce domaine ont alors été rapidement confiées à INTERPOL dont le rôle est la facilitation d’échange de renseignements afin de lutter efficacement contre toute forme de criminalité et notamment la criminalité informatique.



Interpol

Europol est aussi compétente en ce qui concerne la facilitation d’échanges de renseignements entre polices nationales notamment en matière de cybercriminalité. EUROJUST, organe de l’union européenne, a pour compétence l’amélioration de l’efficacité des autorités compétentes des états membres dans la lutte contre la criminalité organisée transfrontalière, donc notamment la cybercriminalité transnationale.

Par ailleurs a été créée en 2004 L’ENISA, agence européenne chargée de la sécurité des réseaux et de l’information, qui a diverses missions, dont notamment le recueil et l’analyse des données relatives aux incidents liés à la sécurité, ou encore le suivi de l’élaboration des normes pour les produits et services en matière de sécurité de réseaux et de l’information, mais aussi la promotion d’activités d’évaluation et de gestion des risques.

Enfin, il existe le programme européen SAFER INTERNET PLUS qui lutte contre les contenus illicites, le traitement des contenus non désirés et préjudiciables, et qui fait la promotion d’un environnement plus sûr.

**Les obstacles à la lutte**

Malheureusement la lutte contre la cybercriminalité n’est pas aisée. Il existe plusieurs obstacles juridiques et non juridiques à cette lutte. En premier lieu, le caractère vaste des réseaux informatiques, mais aussi la rapidité de commission des infractions, la difficulté de rassembler des preuves, et enfin des méthodes d’investigation et de contrôle qui peuvent se révéler attentatoires aux droits fondamentaux, en particulier au droit à l’anonymat et à la liberté d’expression.

Au niveau juridique, ce qui pose aujourd’hui beaucoup de difficultés c’est le fait qu’un même comportement en France et à l’étranger n’est pas pareillement considéré. Il peut constituer une infraction dans un pays et pas dans l’autre. On peut citer pour exemple, la « promotion du cannabis », ou encore la « provocation pour surprendre les pédophiles ». Cela renvoie à un autre problème celui de la loi applicable. En effet, la cybercriminalité « bouleverse le principe classique de la territorialité de la loi pénale ». La loi française sera applicable dès lors qu’un élément constitutif de l’infraction a eu lieu en France (TGI de Paris 17ème chambre, 26 février 2002). Ainsi, par exemple, la simple réception par l’utilisateur est un élément constitutif de l’infraction. Mais s’il n’y a pas d’élément constitutif de l’infraction en France, la loi française ne sera pas applicable.

Il faut alors lutter chaque jour contre les paradis juridiques « cyber paradis », pour une meilleure efficacité du droit relatif à la cyber criminalité.

**Conséquences économiques**

Selon deux études menées par le FBI et IBM en 2006, la cybercriminalité coûterait 67 milliards de dollars par an, rien qu'aux États-Unis4.

Selon le chef d'Interpol Khoo Boon Hui (en), 80 % de la cybercriminalité est liée en 2012 à des bandes organisées transfrontalières et représente un coût financier (750 milliards d'euros par an en Europe) plus important que les coûts combinés des trafics de cocaïne, marijuana et héroïne5.

# Le hacking

Dans un sens large, le **hacking** concerne les activités visant à détourner un objet de sa fonction première. Le hacking a pour fonction de résoudre ou d'aider à résoudre des problèmes, et cela dans de nombreux domaines.



Hacking ou l’art de l’exploitation des failles

Le hacking, quand celui-ci s'apparente au **piratage informatique**1 est une pratique visant à un échange « discret » d'informations illégales et/ou personnelles. Cette pratique établie par les hackers, portion de la population démocratisée en 1983 par le magazine *Newsweek*, émerge lorsque les premiers ordinateurs font leur apparition dans les foyers. Nombre de *crackers* ont commencé leur activité en essayant de casser les restrictions anti-copie ou en détournant les règles des jeux informatiques avant la généralisation d'Internet qui a alors ouvert de plus larges horizons à leur activité. En France, la communauté de hackers s'est plutôt détournée vers le logiciel libre lorsque les médias ont révélé au début des années 1990 que le Chaos Computer Club France était un faux-groupe de hackers qui travaillait en collaboration avec la gendarmerie2, mais de nombreuses communautés indépendantes on vu le jour, et continuent à mettre à disposition leurs ressources, souvent sous forme de wiki ou de repository

En 2009, le hacking regroupe un ensemble de techniques relevant des failles et vulnérabilités d'un élément ou d'un groupe d'éléments, matériel ou humain (*social engineering*). Les attaques informatiques à l'époque de Kevin Mitnick, Kevin Poulsen ou encore Jon Johansen (DVD Jon) étaient peu nombreuses comparées à celles lancées en 2009. De nos jours, la menace est moins virulente, mais beaucoup plus massive, notamment par l'augmentation croissante des « *script kiddies* » ou hacker néophytes.

## Les hackers

Derrière le terme hacker « se cachent des utilisateurs à part, qui préfèrent fouiller dans les entrailles d’un ordinateur plutôt que simplement l’utiliser »3. Les motivations principales du hacker sont « la passion, le jeu, le plaisir, l’échange et le partage »4.

### Pirate ou hacker

De manière générale, les médias modernes semblent relier les hackers informatiques à des pirates informatiques, bien que la traduction de « pirate » ne correspond pas aux définitions de « fouineur » ou de « bidouilleur » que l'on peut trouver dans les institutions qui font référence en langue française.

Le hacking coexiste bien souvent avec la sécurité informatique, mais ces deux domaines ne sont pas à confondre. Cela n'empêche nullement que les hackers soient aussi des spécialistes en informatique.

La différence notable entre ces deux pratiques est que le hacker le fait, normalement, pour aider à "patcher" ces brèches et le pirate le fait dans le but d'exploiter ladite faille.



Pirate ou hacker

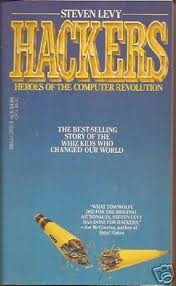
## Le Hacking moderne

Le hacking place les hackers « au cœur du développement de nos sociétés », c'est-à-dire au cœur de l'information et du partage d’information. Cette place au centre du développement des sociétés est surtout due à la curiosité des hackers6. Les hackers utilisent les ressources des communautés de hackers à travers l'échange et le partage pour la résolution d'un problème, on perçoit ce comportement dans le logiciel libre. La résolution se fait souvent en un temps record, car elle se fait par passion, plaisir ou jeu.

### Éthique

L'éthique du hacker a été créée au MIT, et comprend six règles :

* L'accès aux ordinateurs - et à tout ce qui peut nous apprendre comment le monde marche vraiment - devrait être illimité et total.
* L'information devrait être libre et gratuite.
* Méfiez-vous de l'autorité. Encouragez la décentralisation.
* Les hackers devraient être jugés selon leurs œuvres, et non selon des critères qu'ils jugent factices comme la position, l’âge, la nationalité ou les diplômes.
* On peut créer l'art et la beauté sur un ordinateur.
* Les ordinateurs sont faits pour changer la vie.



Steven Levy - Hackers Heroes of the Computer Revolution

« Il n’est pas nécessaire de lire *Hackers*, le livre de Steven Levy, pour réaliser que c'est l'esprit des années 1970 qui souffle dans ces principes. Au MIT, le besoin de libérer l'information répondait à un besoin pratique de partager le savoir pour améliorer les capacités de l'ordinateur. Aujourd'hui, dans un monde où la plupart des informations sont traitées par ordinateur, ce besoin est resté le même - mais il s'étend à tous ceux qui vivent sur cette planète et ont l'intention d'y faire quelque chose, plus seulement aux fondus de l’ordinateur ! »7.

L'auteur de l'éthique du hack moderne invite à ne plus regarder le hacker comme étant uniquement « un étudiant imaginatif et audacieux » ou à « un spécialiste en informatique », mais à étendre cette vision du hacker à l'ensemble de la société et même à la « planète ». Il est rejoint dans son invitation par Le Mentor lorsqu'il dit à la fin de son manifeste « après tout, nous sommes tous pareils ». Selon eux, le hacking doit donc être envisagé dans une vision plus large, et non plus restreinte.

Le hacking a pour fonction de résoudre ou d'aider à résoudre des problèmes, et cela dans de nombreux domaines8. Le hacking comporte plusieurs aspects qui sont l'extension de l'éthique créée au MIT :

* L'*aspect communautaire* forme un des points forts du hacking. L'organisation en communauté permet l’extension du partage d’information, les communautés étant interconnectées la propagation de l'information est très rapide. L'organisation en communauté permet l’entraide entre personnes, mais également aux personnes de jeunes âges qui souhaitent apprendre. L'interconnexion de personnes, qui ne se connaissent pas, permet une aide qui place les individus au même plan, et cela sans jugement de valeur. *Cet aspect pousse à la généralisation et au partage du savoir sans que cela se fasse sur la base de critères tels que « la position, l’âge, la nationalité ou les diplômes ».*
* L'*underground* dans le sens de communauté locale, c'est-à-dire la diffusion de l'information dans un cercle restreint de personnes, on retrouve ce comportement dans le partage de contenu jugé comme illégaux par les autorités, ou encore dans le partage de 0 day. En effet, l'un des aspects du hacking est ce qu'on peut appeler le Warez. Cette attitude ne fait que reprendre l'expression « L’information devrait être libre et gratuite » qui se retrouve également dans le réseau de partage P2P. La communauté locale deviendra globale au fur à mesure que la technologie avancera.
* L'*aspect social*. La dynamique communautaire implique un échange constant d’informations entre les divers acteurs de la communauté. Cet échange demande parfois l’intervention du hacking, et n’est possible que si l’information à échanger inclut une clause de non divulgation. Ainsi le hacking peut forcer pacifiquement l’échange en usant du social engineering qui est la technique qui a le plus d'impact sur la communauté, car elle utilise la « faiblesse humaine »9. L’aspect social se base principalement sur l’échange d’information dans un milieu plus ou moins indépendant.
* L'*aspect technique*. Le hacking regroupe un nombre important de techniques avec plus ou moins de succès, voici quelques-unes des techniques utilisées par les hackeurs : Social Engineering (Ingénierie sociale); Stacks Overflows et Heap Overflows (dépassement de tampon), écriture de shellcode; Exploitation des « format bugs »; Sniffing; Snarfing; Scanning; Spoofing; Hijacking; Fingerprinting; Détournement et utilisation de données WEB (Cookie, CSS, CGI, vulnérabilités concernant les langages PHP, ASP, SQL, etc.); Attaques réseaux qui regroupe Déni de service distribué (DDoS), Attaque de l'homme du milieu (MITM), ARP Spoofing ou ARP Poisoning, Fragments attacks, Tiny Fragments, Fragment Overlapping, IP Spoofing, TCP Session Hijacking, DNS Spoofing, DNS ID Spoofing et DNS Cache Poisoning (empoisonnement du cache DNS)10.

## Hacktivisme

« L'hacktivisme est une contraction de hacking et activisme ». Le fait de hacker et le hacker sont souvent confondus. Cependant, l'acte lui-même de hacker peut être perpétré par tout le monde, ou plutôt toutes personnes voulant un moyen de partager son avis politique. Le terme « hacking », qui est repris dans le monde « hacktivisme », n'est que la représentation que le geste de hacker, mais en aucun cas le personnage même du hacker.

La conséquence la plus fâcheuse est que le hacker souffre de l'hacktivisme parce qu'il apporte auprès des médias une image qui n'est pas la sienne, car les médias confondent encore le fait de hacker et le personnage du hacker6.

## Publications en français

* *Hacker News Magazine*, traduction de *Hacker Journal* (italien), édité par WLF Publishing SRL (Rome), bimestriel, 32 pages, 2 € (France) ;
* *Hackers Magazine*, réalisé par une communauté, édité par WLF Publishing SRL (Rome), bimestriel, 32 pages + 1 CD, 4,99 € ;
* *Hakin9*, publié par Software Sp. z o. o. SK, bimestriel, 84 pages + 1 CD, 7,5 € ;
* *HacKethic*, publié par La Pieuvre Noire, trimestriel, 24 pages grand format
* *L'éthique hacker*, traduction de *The Hacker Ethic* de Pekka Himanen.



Anonymous