**DROIT DE L’INFORMATIQUE**

* **Introduction aux droits de l'informatique :**

Les nouvelles technologies de l'information et de la communication ont mis à l'évidence à leur apparition dans le secteur grand public un manque en matière de législation.

Aujourd'hui, avec la banalisation de l'informatique dans les ménages et l'internationalisation des échanges grâce à internet, certaines personnes clament encore qu'il y a un vide juridique sur internet.

Pour autant il existe de nombreuses lois spécifiques au secteur informatique et lorsqu'un domaine n'est pas traité en particulier par une loi, une analogie est alors faite avec les articles de loi existant dans des domaines similaires et aboutissent généralement à une jurisprudence.

Ainsi le **droit d'auteur** existait avant même que le premier ordinateur soit inventé, mais ce n'est pas pour autant qu'il ne s'applique pas aux œuvres numériques ou numérisées.

Concernant les intrusions non autorisées sur un système informatique (à travers internet ou non) **la loi Godfrain** du 8 janvier 1988 prévoit un cadre pénal prévoyant des infractions spécifiques en fonction de l'atteinte portée au système informatisé. reprises par les articles 323-1 à 323-7 du nouveau code pénal institué par La loi du 22 juillet 1992 entrée en vigueur le 1er mars 1994 a ainsi institué la reprise de ces infractions dans les articles 323-1 à 323-2 du nouveau code pénal.

D'autre part, la nature même des informations traitées par les technologies de l'information et de la communication rend les données personnelles encore plus sensibles. Ainsi une loi a été écrite spécifiquement pour protéger les données personnelles afin de respecter le droit de liberté individuelle. Sont ainsi sanctionnés pénalement tout manquement à mettre en œuvre un mécanisme de protection adapté aux données stockées.

* Protection des créations informatique,
* **La propriété intellectuelle :**

Le terme de **propriété intellectuelle** est présent dans le droit français (le **Code de la propriété intellectuelle**). Il est un calque direct de l'anglais, *intellectual property*.

Dans son acception courante, il recouvre les droits d'utilisation d'une « **création intellectuelle** » : invention, solution technique, œuvre littéraire ou artistique, marque, dessins et modèles industriels, logiciels, circuits intégrés, etc. Précisons tout de suite que les découvertes scientifiques sont exclues de toute protection relevant de la propriété intellectuelle.

Bien entendu, les divers éléments qui composent la propriété intellectuelle ont un régime juridique différent dû à leur nature même.

On inclut généralement sous l'expression "**propriété intellectuelle**" deux branches principales : la **propriété industrielle** et la propriété littéraire et artistique.

\* Pour fixer les idées, on peut dire que la **propriété industrielle** concerne, grosso modo, les marques, les **brevets,** les inventions, les **dessins et modèles industriels**, les **appellations d'origine** et les indications de provenance.

\* La **propriété littéraire et artistique** s'explique d'elle-même ; toutefois on y a agrégé d'autres éléments sur lesquels nous reviendrons.

Propriété industrielle et propriété littéraire et artistique sont régies par les principes généraux du droit de la propriété tels qu'édictés par les codes civils et par les textes particuliers qui leur sont applicables.

Il faut signaler que les dessins et modèles industriels ont un statut hybride en droit français, entre **propriété intellectuelle** et propriété littéraire et artistique. Ce statut est en cours de généralisation dans l'[Union européenne](http://fr.wikipedia.org/wiki/Union_europ%C3%A9enne).

* **Droit d’auteur**

Le droit d'auteur en France est régi par la loi du 11 mars 1957 et la loi du 3 juillet 1985, codifiées dans le **code de la propriété intellectuelle**.

La loi reconnaît en tant qu'auteur toute personne physique qui crée une œuvre de l'esprit quelle que soit son genre (littéraire, musical ou artistique), sa forme d'expression (orale ou écrite), son mérite ou sa finalité (but artistique ou utilitaire).

Le droit d'auteur couvre donc toute création de l'esprit, qu'elle soit une œuvre littéraire (livres, journaux, pièces de théâtre, logiciels, site web, etc.), une œuvre d'art (peinture, sculpture, photographie, image infographiée, architecture, etc.), une œuvre musicale ou audiovisuelle, dès lors qu'elle est **matérialisée**, **originale** et qu'elle est l'**expression de la personnalité de l'auteur**. Ainsi ne tombent pas sous la protection du droit d'auteur les créations de l'esprit purement conceptuelles telles qu'une idée, un concept, un mot du langage courant, ou une méthode.

D'après les articles L.111-1 et L.123-1 du code de la propriété intellectuelle, l'auteur d'une œuvre de l'esprit jouit d'un droit de propriété exclusif dès sa création, sans nécessité d'accomplissement de formalités (dépôt ou enregistrement), pour une durée correspondant à l'année civile du décès de l'auteur et des soixante-dix années qui suivent, au bénéfice de ses ayants-droits. Au-delà de cette période, les œuvres entrent dans le **domaine public**. Toutefois, en cas de litige, il est nécessaire de pouvoir apporter une preuve de l'existence de l'œuvre à une date donnée, soit en ayant effectuée préalablement un dépôt auprès d'un organisme habitilité, soit en ayant rendue l'œuvre publique et en étant en moyen de le prouver.

**Article L. 111-1 du Code de la propriété intellectuelle** :

 L'auteur d'une œuvre de l'esprit jouit sur cette œuvre, du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous.

 Ce droit comporte des attributs d'ordre intellectuel et moral, ainsi que des attributs d'ordre patrimonial [...].

**Article L. 123-1 du Code de la propriété intellectuelle** :

 L'auteur jouit, sa vie durant du droit exclusif d'exploiter son œuvre sous quelque forme que ce soit et d'en tirer un profit pécuniaire.

 Au décès de l'auteur, ce droit persiste au bénéfice de ses ayants-droits

Le code de la propriété intellectuelle distingue en réalité deux types de droits :

* le droit patrimonial s'exerçant pendant toute la vie de l'auteur et transmissible à ses héritiers les 70 années suivantes ;
* le droit moral reconnaissant la paternité d'une œuvre à son auteur sans limite de durée.

Le **droit moral** permet à l'auteur de jouir du droit au respect de son nom, de sa qualité et de son œuvre. Il s'agit d'un droit **imprescriptible** (c'est-à-dire d'une durée illimitée), **inaliénable** (il ne peut être cédé à un tiers) et **perpétuel** (il est transmissible aux héritiers) le droit moral.

Ainsi, lorsqu'une œuvre tombe dans le domaine public, il est impératif lors de son utilisation de citer son nom et celui de son auteur ainsi que d'en respecter l'intégrité, au risque sinon de se voir réclamé des dommages et intérêts par les héritiers !

Le **droit patrimonial** est le droit exclusif d'exploitation accordé à l'auteur, lui permettant éventuellement d'en tirer un profit par cession de :

* **droit de représentation**, permettant d'autoriser ou non la diffusion publique de l'œuvre. Sont notamment cités à titre d'exemple dans le *code de la propriété intellectuelle* la récitation publique, la présentation publique, la projection publique, la télédiffusion, mais la diffusion au travers de réseau informatique rentre dans ce même cadre.
* **droit de reproduction**, permettant d'autoriser ou non la reproduction de l'œuvre.

Les droits de représentation et de reproduction sont cessibles par contrat écrit rédigé par l'auteur précisant les conditions et la durée de la session des droits. La session des droits sur une œuvre peut ainsi conduire à une rémunération obligatoirement proportionnelle aux recettes de l'exploitation.

**Limite :**

Des exceptions existent tout de même lorsque l'œuvre est divulguée, c'est-à-dire que l'auteur ne peut s'opposer à :

* la **représentation privée et gratuite dans un cercle de famille** ;
* la **copie ou reproduction réservée à un usage strictement privé** du copiste ;
* la **publication d'une citation** ou d'une analyse de l'œuvre, dans la mesure où celle-ci est brève et justifiée par le caractère critique, polémique, pédagogique, scientifique ou d'information, de l'œuvre ;
* la parodie et la caricature.
* **Protéger ses créations :**

Il vous est sûrement déjà arrivé de craindre (ou de constater) que quelqu'un s'approprie des œuvres que vous avez publiées (sur [internet](http://www.commentcamarche.net/internet/internet.php3) ou tout autre support) afin de mettre à son profit vos créations.

Il est impossible d'empêcher des personnes de copier, il existe cependant des moyens légaux de les dissuader ou bien de faire jouer la justice**.**

**Comment empêcher le pillage ?**

A partir du moment où un webmaster diffuse sur internet des informations (images, textes, sons, vidéos, etc.), il s'expose évidemment au pillage de son contenu par des internautes peu respectueux ou méconnaissant le [droit d'auteur](http://www.commentcamarche.net/droits/copyright-auteur.php3) en vigueur en France.

Il existe certes des dispositions techniques permettant de limiter le risque de copies abusives en empêchant par exemple au maximum l'internaute d'avoir accès au code source de la page web. Toutefois il est impossible d'empêcher à 100% la copie dans la mesure où  :

Tout ce qui s'affiche à l'écran est potentiellement copiable

* **La protection des logiciels :**

Cette rubrique s'intéresse plus particulièrement aux aspects de protection des logiciels, à l'exploitation des licences ainsi qu'à la brevetabilité des logiciels:

* **La protection des logiciels par le droit d'auteur**
* **Les modalités de la protection**
* **Les différents types de dépôts**
* **La protection du nom du logiciel : application du droit des marques**
* **L'exploitation des logiciels : les licences**
* **La brevetabilité du logiciel**
* **Le contexte international**

**La protection des logiciels par le droit d'auteur :**

Depuis la loi du 3 juillet 1985 qui a étendu la notion d'œuvre de l'esprit aux logiciels, le logiciel est protégé par le droit d'auteur. L'ensemble du dispositif législatif applicable aux logiciels est aujourd'hui intégré dans la première partie du Code de la propriété intellectuelle, parmi les dispositions relatives à la propriété littéraire et artistique.

**Les modalités de la protection :**

  **Les conditions de la protection :**

Seuls les logiciels présentant un caractère original sont protégés par le droit d'auteur.

Le critère d'originalité est la seule condition de fond nécessaire à la protection du logiciel par le droit d'auteur. Ce critère d'originalité n'est pas défini par la loi. Il convient de se référer à la jurisprudence PACHOT (Cass, Assemblée plénière, 7 mars 1986) selon laquelle "l'originalité d'un logiciel consiste dans un effort personnalisé allant au-delà de la simple mise en œuvre d'une logique automatique et contraignante". Cela ramène la notion d'originalité à la "marque d'un apport intellectuel".

**L'objet de la protection :**

La protection du logiciel ne s'étend pas aux idées qui sont à la base du logiciel. Seule la mise en forme de ces idées peut faire l'objet d'une protection par le droit d'auteur.

  Les éléments du logiciel non protégés :

* Les fonctionnalités
* Les algorithmes
* Les interfaces
* Les langages de programmation

Tous ces éléments sont en effet considérés comme des éléments informatiques à l'origine de la conception du logiciel ne présentant pas en tant que tels une forme définie. Ils appartiennent au domaine de l'idée.

La documentation d'utilisation du logiciel sur papier (protégée par le droit d’auteur traditionnel, en tant qu’œuvre distincte du logiciel)

  Les éléments protégés

* L'architecture des programmes
* Le code source
* Le code objet (résultat de la compilation du code source)
* Les différentes versions
* Les écrans et modalités d'interactivité s'ils sont originaux
* Le matériel de conception préparatoire (Art. L.122-2 du CPI) : les ébauches, les maquettes, les dossiers d'analyses fonctionnelles, la documentation de conception intégrée au logiciel, les prototypes.

**Les techniques de protection :**

 Absence de formalités :

Un logiciel original est protégé par le droit d'auteur, du seul fait de sa création.

Cette protection n'est soumise en France à aucune procédure particulière, l'apposition de la mention Copyright, n’est donc pas nécessaire. Cependant, malgré son absence de fondement légal, dans le cadre d’une exploitation large du logiciel, on ne peut que recommander d’apposer la mention Copyright, car nombre de législations étrangères exigent l'accomplissement de cette formalité pour les œuvres publiées dont les logiciels exploités.

Intérêt du dépôt :

Si aucune formalité de dépôt de l'œuvre n'est imposée, le dépôt du logiciel peut néanmoins présenter un intérêt pour pré-constituer la preuve de la création et lui donner date certaine, en cas notamment de contestation future.

**Les différents types de dépôts** :

**Auprès de qui peut-on déposer ?**

Théoriquement, le dépôt peut être effectué chez tout tiers habilité à le recevoir et lui conférer date certaine. Il est même possible de s'adresser un courrier à soi-même ce qui peut s'avérer utile (et économique) pour conserver les versions successives non définitives d'un logiciel.

Les officiers ministériels (notaire ou huissier) sont habilités à recevoir ce genre de dépôt. Ils apposent des scellés, consignés par procès verbal et conservent sous séquestre les biens confiés en dépôt. Dans la pratique, peu de dépôts s'opèrent de la sorte, les officiers ministériels hésitant à traiter ce type de dossier.

De même, il est possible de déposer un logiciel à l'INPI, sous enveloppe Soleau, mais cette pratique n'est pas adaptée au logiciel, en raison du format de l'enveloppe et des risques de perforation.

Il existe enfin des sociétés de gestion collective des droits d'auteur, organismes chargés de collecter et répartir les droits d'auteur, dont certaines acceptent les dépôts de logiciels. La Société des gens de lettres de France en fait partie et elle accepte les logiciels sous forme de scénario ou d'organigramme. Peu contraignante (enveloppe cachetée à la cire ou apposition de signature sur le pli de fermeture, avec indication du nom de l'auteur et du titre de l'œuvre), cette méthode est cependant peu adaptée au dépôt des logiciels, puisqu'elle ne prévoit pas les modalités d'accès aux sources par des tiers.

**La protection du nom du logiciel : application du droit des marques**

En tant qu'œuvre, le nom du logiciel est protégé par le droit d'auteur. Si un dépôt du logiciel est effectué auprès de l'APP, le nom de ce logiciel est protégé.

Pour les projets d'une certaine ampleur (lourds investissements prévus, création d'un site Web, renommée des entités participantes, lourdes communications envisagées sur le projet) il est recommandé de protéger le nom du logiciel par un dépôt de marque et d'enregistrer dans certains cas le nom de domaine correspondant.

Dans tous les cas, il convient de s'être assuré, par une première recherche d'antériorités, de la disponibilité de la marque et du nom de domaine.

L'exploitation des logiciels : les licences :

  Le choix de la licence

Le titulaire des droits patrimoniaux d'un logiciel a la possibilité d'en concéder l'exercice à un tiers. Dans cette hypothèse il va définir par le biais d'un document contractuel dénommé "licence", l'étendue des droits qu'il concède au licencié. Cette licence peut ainsi aller de la simple concession du droit d'usage du logiciel sur un seul ordinateur et pour une durée limitée à des fins d'évaluation, à une licence très large permettant à celui qui en bénéficie de reproduire le logiciel et de le distribuer librement dans le commerce. Toutes les restrictions sont possibles sous réserve des dispositions de l'article L.122-6 -1 du CPI et notamment du droit pour le licencié de réaliser une copie de sauvegarde du logiciel.

Une catégorie particulière : la licence de logiciel libre

On désigne comme "libre" un logiciel disponible sous forme de [code source](http://www.sg.cnrs.fr/daj/propriete/logiciels/logiciels5.htm) (différent de [code exécutable](http://www.sg.cnrs.fr/daj/propriete/logiciels/logiciels5.htm)) c'est à dire un logiciel dont l'architecture interne est partagée et diffusée librement. L'utilisateur d'un logiciel dit "libre" est autorisé à le modifier, le corriger, l'adapter.

Pour la majorité de la doctrine, le créateur d'un tel logiciel n'abandonne pas ses droits d'auteur mais concède seulement à chacun le droit d'utiliser son œuvre à condition que toutes les améliorations soient rendues publiques et que le logiciel ainsi modifié circule librement.

 Le logiciel libre (différent du [logiciel propriétaire](http://www.sg.cnrs.fr/daj/propriete/logiciels/logiciels5.htm)) ne doit donc pas être confondu avec :

* le logiciel dans le domaine public sur lequel l'auteur a renoncé à tous ses droits
* le freeware, logiciel gratuit mais pas nécessairement libre
* le shareware, logiciel dont l'utilisation est soumise à rétribution de l'auteur, après une période d'essai gratuite.

En revanche un logiciel libre peut être un [logiciel commercial](http://www.sg.cnrs.fr/daj/propriete/logiciels/logiciels5.htm).

L'auteur d'un logiciel qui sera qualifié de "libre" concède donc à l'utilisateur un droit d'usage et de modification de son œuvre mais dans un cadre juridique spécifique c'est-à-dire par le biais de licences.

Il existe un certain nombre de modèles de licence adaptés aux logiciels libres, l'une des plus utilisée par la communauté scientifique étant la licence [GNU GPL](http://www.sg.cnrs.fr/daj/propriete/logiciels/logiciels5.htm) (General Public Licence).

Le CNRS, le CEA et l'INRIA se sont associés récemment pour élaborer une licence de logiciel libre conforme au droit français.

**La brevetabilité du logiciel :**

**Une protection indirecte en Europe :**

La convention de Munich sur la délivrance de brevets européens du 5 octobre 1973 et l'article L.611-10.2 c) du Code de la propriété intellectuelle excluent expressément les logiciels du domaine de la brevetabilité.

Cependant cette exclusion ne concerne que les programmes "en tant que tels". Une demande de brevet ne peut revendiquer un logiciel à titre principal, mais peut porter sur une invention comportant un programme d'ordinateur qui se présente comme une étape de fonctionnement de l'invention revendiquée.

La position de l'Office Européen des Brevets (OEB) est maintenant claire sur ce point : le critère retenu pour analyser si une invention est exclue de la brevetabilité est "la contribution à l'état de la technique de l'invention (telle que définie dans la revendication) considérée dans son ensemble". En appliquant ce critère, on arrive donc à séparer deux catégories de "programmes d'ordinateurs" :

* les programmes d'ordinateur dont la mise en œuvre produit des caractéristiques techniques nouvelles et inventives et qui de ce fait sont brevetables
* les programmes d'ordinateur pris en tant que tels (qui n'ont aucun rapport avec la technique) et qui sont exclus de la brevetabilité.

**Le contexte international**

 Aux États-Unis, l'office des brevets USPTO a adopté une pratique favorable à la protection par brevet des programmes d'ordinateurs, y compris de programmes d'ordinateurs ne produisant pas d'effet technique. On estime qu'environ 12 000 brevets de logiciels sont déposés chaque année aux États- unis. Aujourd'hui, les brevets de logiciels représentent 15% des brevets déposés aux État-Unis.

Au Japon, l'office des brevets a adopté en 1997 des lignes directrices favorables à la protection des logiciels et l'on compte aujourd'hui environ 20 000 brevets japonais portant sur des logiciels.

* **Protection des données**

Tout ordinateur est appelé à échanger avec l'extérieur : connexion Internet (pages web, messagerie...), connexion réseau, lecteurs divers (disquette, cédérom, clé USB...). Lors de ces échanges, il existe un risque de contact avec des éléments malveillants : les virus sont les plus connus de ces dangers mais il en existe d'autres.

Ces agressions sont le fait d'informaticiens très avertis, maîtrisant parfaitement la programmation. Elles se manifestent sous forme de fichiers informatiques dont les actions sont diverses mais toujours nuisibles à votre ordinateur : ralentissement voire blocage de la machine, suppression de documents, modifications de programmes, diffusion d'informations privées...

* **Virus**

**Risques**
Un virus informatique est un programme conçu pour se dupliquer ; il se propage par tous les moyens d'échange de données numériques (Internet, réseau, disquette, cédérom, clé USB…) ; les effets d'un virus sont très variés, de l'affichage d'un simple message anodin à la destruction complète de toutes les données de l'ordinateur.

**Protections**Les antivirus sont des logiciels conçus pour repérer les traces d'activité des virus, les bloquer et isoler ou supprimer les fichiers qui en sont responsables. Leur mode de fonctionnement est basé sur une veille permanente, à deux niveaux :

* sur tout ordinateur, un programme antivirus doit être installé et actif.
* cet antivirus doit être tenu à jour : la surveillance par l'antivirus se réfère à une base de données contenant les signes d'activité de tous les virus connus. Chaque jour, de nouveaux virus apparaissent, inventés par des experts en programmation désireux d'éprouver leurs compétences ; en permanence, d'autres experts surveillent l'apparition de ces nouveaux programmes et conçoivent des antidotes. On comprend qu'un antivirus ne sera efficace que s'il est régulièrement actualisé, pour détecter les manifestations de tous les nouveaux virus.
* **Chevaux de Troie / backdoors**

**Risques**Voisin des virus, un cheval de Troie (aussi appelé troyen ou trojan) est un programme qui, sous les apparences d'un logiciel utile, autorise l'exécution de commandes sur votre ordinateur, depuis un ordinateur distant, via Internet.

Certains chevaux de Troie, les backdoors, permettent de contrôler à distance votre ordinateur : après avoir infecté votre machine (lors du téléchargement d'un fichier ou l'ouverture d'une pièce jointe), le programme permet, lorsque vous êtes en connexion Internet, d'avoir un accès libre en lecture, écriture ou suppression à la totalité des fichiers présents sur votre disque dur mais également de faire exécuter à votre ordinateur des actions illégales (attaques de serveurs, intrusions dans des sites sensibles…).

**Protections**Un antivirus (à jour) permet de limiter les risques d'infection.

Un firewall (matériel ou logiciel) permet, en plus, de surveiller le trafic sur votre accès Internet, pour détecter les tentatives de connexion non volontaires. En cas d'accès permanent (ADSL), il est indispensable d'utiliser un firewall qui filtre le trafic entre votre réseau local et Internet.

* **Spyware**

**Risques**Un spyware (ou logiciel espion) est un programme conçu pour collecter des données personnelles sur son utilisateur et les envoyer, à son insu, à un tiers via Internet.
Les spywares ne sont pas des virus parce qu'ils ne mettent pas en danger l’intégrité du système, des applications et des données. Mais leurs actions posent des problèmes éthiques et juridiques, quant à la violation de la vie privée.

Les adwares sont des spywares qui utilisent les données récoltées (pages web visitées, essentiellement) pour afficher des publicités ou envoyer des mails ciblés ; certains sont capables de modifier la page par défaut de votre navigateur.

Les spywares sont généralement inclus dans des logiciels utilitaires : logiciels P2P (Kaaza, e-Mule…), lecteurs de médias (DivX) en sont des vecteurs connus. Mais certains fabricants de matériels et de logiciels commerciaux en incluent dans leurs produits.

Les cookies sont également des fichiers qui recueillent des informations sur la navigation des internautes mais ils ne servent qu'à faciliter la navigation dans un site donné ; ils restent, en principe, stockés sur le disque dur de l'utilisateur et ne sont pas transmis à des tiers.

**Protections**La relative innocuité des spywares a conduit les fabricants d'antivirus à les négliger et des logiciels spécifiques souvent gratuits se sont développés. Les anti-spywares, comme les antivirus, utilisent des bases de données fréquemment mises à jour.

* sur tout ordinateur, un anti-spyware doit être installé et actif.
* cet anti-spyware doit être tenu à jour : la plupart des anti-spywares sont actualisables en ligne,
* sur le site de leur éditeur.
* **Spams**

**Risques**

Le spam (ou pourriel) désigne l'envoi massif de courriers électroniques, sans sollicitation des destinataires, à des fins publicitaires ou malhonnêtes. C'est un phénomène d'ampleur puisqu'on estime que 30 à 40% des mails circulant sur Internet seraient des spams.

Il existe un important trafic souterrain de listes d'adresses électroniques qui permet à des ordinateurs d'adresser un nombre énorme de mails en peu de temps.

Les produits les plus vantés sont les sites pornographiques, les médicaments, le crédit financier ou des escroqueries prétendant enrichir rapidement. Une autre forme de spam (appelée phishing) consiste à tromper le destinataire en faisant passer le message pour un message de sa banque ou d'un quelconque service protégé par mot de passe. Le but est de récupérer les données personnelles des destinataires (notamment des mots de passe) en les attirant sur un site factice enregistrant leurs actions.

**Protections**

Il est difficile, au niveau de l'utilisateur, de lutter contre les spams ; quelques mesures de prévention sont, toutefois, possibles :

- ne pas donner son adresse mail sur un site inconnu

- ne pas répondre aux messages de spam ni cliquer sur les liens qui prétendent vous désabonner de ces courriers.

Les serveurs de messagerie des fournisseurs d'accès Internet sont équipés de logiciels antispams qui analysent les messages et limitent l'arrivée, dans votre ordinateur, de ce type de mails.

* **Hoaxes**

**Risques**Il existe de faux virus, appelés hoaxes : un hoax se présente, en général, sous la forme d'un mail d'alerte contre un nouveau virus ; le message se réclame souvent d'un fabricant connu d'antivirus ou de matériel informatique, il signale un fichier dangereux et vous conseille de le détruire et demande qu'on diffuse largement l'information.

Le but des hoaxes est le simple plaisir, pour leurs concepteurs, de constater l'affolement et les encombrements provoqués par leur "plaisanterie".

**Protections**Lors de la réception d'un message douteux de ce type, avant de supprimer un fichier essentiel de Windows et d'alerter tout votre carnet d'adresses, renseignez-vous… On peut trouver, sur Internet, des sites d'information sur ces fausses alertes.

* **Problèmes utilisateurs**

**Risques**Les utilisateurs, eux-mêmes, peuvent être à l'origine de pertes de données : par malveillance (peu fréquent, dans le cadre scolaire, beaucoup plus en entreprise) ou par maladresse. Documents non enregistrés, effacés ou perdus lors de manipulations hasardeuses sont source d'importantes pertes de temps et d'animosité à l'égard de l'outil informatique.

**Protections**La protection contre ce risque passe par une connaissance de base du fonctionnement d'un ordinateur et, en particulier, du système de fichiers (notions d'arborescence, dossier, fichier…). Des habitudes efficaces et bien maîtrisées de création et d'enregistrement des documents sont indispensables : création des documents directement dans un dossier adapté, enregistrement à intervalles réguliers pendant le travail, maîtrise des opérations de copier/couper/coller limitent les risques de fausse manœuvre.

* **Mots de passe**

**Risques**Un certain nombre de ressources sont protégées par mots de passe pour garantir que leur utilisation reste le fait de personnes autorisées : accès à un ordinateur voire à certains dossiers et fichiers, connexion Internet, accès à une boîte de messagerie, accès à certaines pages web…
Le vol de mot de passe (par simple lecture s'il est placé à un endroit trop facilement accessible ou par "devinette" s'il est trop simple) permet à un usager non autorisé d'accéder à des outils ou à des données qui ne le concernent pas ; l'usage qu'il peut en faire serait alors imputé à l'utilisateur dont il a usurpé le mot de passe.

**Protections**Le caractère relativement peu sensible des données d'une école ne nécessite pas une politique très contraignante en matière de mots de passe. Mais un minimum de sécurité et de confidentialité est recommandé :

* l'accès à l'ordinateur de gestion devra être protégé par un mot de passe puisqu'il contient des données confidentielles sur les élèves.
* ce mot de passe ne sera pas affiché sur un post-it, collé sur l'ordinateur…

Pour des raisons de sécurité mais aussi de re-paramétrage en cas de problème, il est prudent de conserver l'ensemble des mots de passe de l'école en lieu sûr (nom d'utilisateur et mot de passe, qui vont ensemble, pour la connexion Internet, les boîtes de messagerie et les accès aux ordinateurs protégés).

* **Partages**

**Risques**L'intérêt principal d'un réseau est le partage des ressources : dossiers et fichiers, accès Internet, imprimantes… Par défaut, lors de l'installation d'un réseau, rien n'est partagé, ce qui permet de n'ouvrir à l'accès depuis une autre machine que pour les ressources souhaitées, en les protégeant éventuellement par un mot de passe. Les risques liés aux partages sont de deux types :

* accès à des données confidentielles par des utilisateurs locaux non autorisés.
* accès à ces mêmes données et/ou prise de contrôle à distance depuis un ordinateur extérieur, via la connexion Internet.

**Protections**Le partage complet des imprimantes est sans danger ; le partage de connexion Internet se met en place lors de la configuration du réseau et n'a pas à être restreint sauf si on souhaite interdire la sortie à une machine particulière ; quant au partage de dossiers, il est à définir en fonction des contenus et des utilisateurs susceptibles d'y accéder.
Il est possible d'activer le partage complet des disques des postes "élèves", ce qui facilite les transferts de fichiers ; il est cependant plus prudent de limiter ce partage à un dossier, appelé, par exemple "documents partagés", dans lequel on pourra créer autant de sous-dossiers que nécessaire, pour éviter l'accès aux dossiers système de la machine.
Pour le poste de gestion, il peut être utile de créer un dossier partagé qui permettra des échanges avec les autres postes mais il est indispensable de ne pas partager le reste du disque pour en préserver la sécurité et la confidentialité.

* **Sauvegarde**

**Risques**Malgré toutes les précautions prises contre les risques évoqués plus haut, il peut arriver que des données soient perdues ; le temps mis à les créer, la complexité de leur élaboration, leur caractère vital sont autant de facteurs aggravants de cette perte ; c'est pourquoi le recours à des procédures de sauvegarde est indispensable, au moins pour les données essentielles : il s'agit de conserver, en lieu sûr, une copie de ces données.

**Protections**Une sauvegarde n'a de sens que si elle est :

* rigoureuse : il faut donc définir précisément les fichiers à sauvegarder ; ceci suppose une connaissance du système de fichiers de l'ordinateur et une gestion assez rigoureuse lors de l'enregistrement de vos documents. La sauvegarde de la messagerie demande de savoir localiser les fichiers qui la composent. Faute de ces connaissances, la sauvegarde sera probablement incomplète (la sauvegarde d'un disque dur entier est irréaliste).
* à jour : donc assez fréquente pour sauvegarder la dernière version de chaque document.
* récupérable : il s'agit donc d'utiliser un support et un logiciel appropriés et de les avoir testés avant d'avoir besoin d'une vraie restauration de données.

# Introduction à la criminalité informatique

**Présentation générale**

Les réseaux numériques – singulièrement l’internet – peuvent être l’instrument d’abus relativement spécifiques, en ce sens qu’ils ont pour cibles des biens de l’informatique. On parle, dans ce cas, de « criminalité informatique », à moins d’utiliser un néologisme dans le vent tel que cybercriminalité (ou cyberterrorisme).

Les comportements répréhensibles sont diversifiés : entrée par effraction dans un système informatique, manipulation ou destruction de données, pillage de données, piratage de programmes, envoi d’un virus, etc.

Mais, l’internet est aussi le support d’infractions tout à fait conventionnelles, qui peuvent se commettre par d’autres moyens : atteintes à l’honneur et à la bonne réputation (diffamation, calomnie...); atteintes à la vie privée ; escroqueries (cf. *phishing*, « vol d’identité » ou « hameçonnage » ; « lettres nigérianes »…); violation de secrets professionnels (art. 458 C. pén.); pédopornographie ; propos racistes, révisionnistes, négationnistes ou violents; contrefaçon de droits de propriété industrielle ou intellectuelle; violation du secret de l’instruction, du droit à l’image; etc.

Une criminalité relativement originale donc, et une criminalité plus classique, qui tire parti de la couverture mondiale du nouveau média.

Notre droit pénal est globalement apte à protéger les utilisateurs de l’internet contre ceux qui s’en servent pour commettre des infractions classiques. Plusieurs infractions tombent clairement sous l’application de dispositions du Code pénal formulées en termes suffisamment larges. Ainsi, il est clair que celles concernant les atteintes portées à l’honneur ou à la considération des personnes (art. 443 et s.) s’appliquent aux messages à caractère calomnieux, diffamatoire ou injurieux véhiculés par l’internet. Les dispositions relatives à la corruption de la jeunesse (art. 379 et s.) visent pareillement toute une série d’abus (incitations à la débauche de mineurs, promotion de la pédophilie, publicité en faveur du tourisme sexuel...) sans opérer de distinction entre les supports de cette diffusion.

En revanche, pour faire face aux infractions d’un nouveau genre apparues avec les développements de l’informatique et des réseaux, notre pays était désarmé. A cet égard, le « vide juridique » a été comblé, il y a peu, par l’adoption de la loi du 28 novembre 2000 relative à la criminalité informatique. Cette loi a subi quelques retouches suite à l’adoption de la loi du 15 mai 2006 modifiant les articles 259*bis*, 314*bis*, 504*quater*, 550*bis* et 550*ter* du Code pénal.

Une difficulté particulière vient du fait que le droit pénal est, par essence, un droit national, alors que l’internet est un phénomène sans frontière. Des règles existent certes pour résoudre d’évidents conflits de lois (quelle loi appliquer ?) et de juridictions (quel est le tribunal compétent ?). Mais on devine aisément combien leur mise en œuvre se heurtera souvent à d’insurmontables obstacles pratiques : difficultés d’identification de l’émetteur du message litigieux, possibilité d’œuvrer à partir d’un paradis électronique (entendez : où la loi pénale est plus laxe...), inutilité d’une sanction frappant un individu résidant à l’autre bout du monde, etc.

En théorie, la loi pénale belge est applicable à toutes les infractions commises sur le territoire du Royaume (art. 3 C. pén.). C’est le principe, bien connu, de territorialité du droit pénal : dès que quelqu’un – Belge ou étranger, peu importe sa nationalité – commet une infraction sur le territoire de la Belgique, il peut être poursuivi et le juge saisi statuera selon le droit belge. La jurisprudence considère, plus précisément, que le juge belge est compétent pour statuer sur une infraction dès l’instant où l’un de ses éléments constitutifs a été réalisé sur le territoire belge (principe dit de l’ubiquité).

En revanche, l’infraction commise hors du territoire du Royaume par des belges ou par des étrangers n’est punie en Belgique que dans les cas déterminés par la loi (art. 4 C. pén.). Sauf circonstances exceptionnelles (atteintes à la sûreté de l’Etat...), les infractions commises à l’étranger ne sont poursuivies que si l’inculpé est appréhendé en Belgique. Souvent aussi, la compétence du juge est soumise au principe de la double incrimination.

Supposons qu’un message à caractère raciste ou incitant à la violence soit « lancé » sur le réseau à partir de l’Allemagne et reçu en Belgique. On peut penser que, dans ce cas, l’incitation à la haine ou à la violence est réalisée en Belgique de sorte qu’un élément constitutif de l’infraction est bien localisé sur le territoire du Royaume. Le juge belge est donc compétent pour statuer sur l’infraction sur la base de l’article 3, c’est-à-dire sans que les conditions plus strictes de l’article 4 (double incrimination, présence de l’inculpé sur le territoire du Royaume...) doivent être remplies. Cette solution s’inspire de la jurisprudence selon laquelle, en cas d’infractions commises à la radio ou à la télévision, « l’infraction est supposée accomplie en tout lieu où pareille diffusion a pu être reçue ou entendue ».

En bref, on a beau dire qu’une infraction reste telle même si elle est perpétrée dans « l’espace virtuel », il est tout de même permis de se demander si les Etats auront toujours les moyens de faire respecter leur loi pénale. Apparaît ainsi la nécessité de renforcer la coopération entre Etats (pour favoriser les extraditions, l’*exequatur* des décisions de justice étrangères, la collaboration judiciaire et policière...). Mais il ne faut pas se leurrer : la route promet d’être longue tant sont importantes les différences de valeurs et de sensibilités d’un pays à l’autre. De toute évidence, les libertés les plus élémentaires — notamment la très concernée liberté d’expression — ne sont pas conçues de la même façon, loin s’en faut, en Chine, en Algérie, aux Etats-Unis, en Europe, en Corée, au Congo...

Les pages qui suivent visent à présenter les nouvelles dispositions introduites dans le Code pénal et dans le Code d’instruction criminelle par la loi du 28 novembre 2000 relative à la criminalité informatique. L’exposé portera essentiellement sur l’analyse des nouvelles infractions informatiques (I.). L’adaptation des règles de procédure pénale à la lutte contre la cybercriminalité fera l’objet d’un examen plus sommaire (II.).

**I. Les nouvelles incriminations informatiques**

La loi du 28 novembre 2000 vient enrichir notre Code pénal de nouvelles incriminations : le faux en informatique, la fraude informatique et les « infractions contre la confidentialité, l’intégrité et la disponibilité des systèmes informatiques et des données qui sont stockées, traitées ou transmises par ces systèmes ».

Ces dernières infractions – reprises au titre IX*bis* nouveau du Code pénal (introduit par l’art. 6 de la L. 28 nov. 2000) – visent en réalité deux catégories d’infractions : l’accès et le maintien non autorisé dans un système (*hacking*) et le sabotage informatique.

Nous examinons, tour à tour, ces différentes infractions nouvelles.

### 1. Le faux en informatique

 **Art. 210*bis.*** **§ 1er.** Celui qui commet un faux, en introduisant dans un système informatique, en modifiant ou effaçant des données, qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation possible des données dans un système informatique, et par là modifie la portée juridique de telles données, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de vingt-six euros à cent mille euros ou d'une de ces peines seulement.

**§ 2.** Celui qui fait usage des données ainsi obtenues, tout en sachant que celles-ci sont fausses, est puni comme s'il était l'auteur du faux.

**§ 3.** La tentative de commettre l'infraction visée au § 1er est punie d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à cinquante mille euros ou d'une de ces peines seulement.

**§ 4.** Les peines prévues par les §§ 1er à 3 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans qui suivent le prononcé d'une condamnation pour une de ces infractions ou pour une des infractions prévues aux articles 259*bis*, 314*bis*, 504*quater* ou au titre IX*bis*.

L’infraction de faux en informatique vise la dissimulation intentionnelle de la vérité par le biais de manipulations informatiques de données pertinentes sur le plan juridique. Des données sous forme électronique peuvent être ainsi falsifiées moyennant modification ou effacement (complet ou partiel), lors de leur saisie (introduction dans l’ordinateur), de leur récupération ou au cours de leur stockage. En incriminant celui qui se rend coupable d’un faux en informatique, le nouvel article 210*bis* permet d’obvier aux hésitations doctrinales et jurisprudentielles quant à l’application aux données électroniques des articles 193 et suivants du Code pénal relatifs au faux en écriture.

Selon les travaux préparatoires de la loi du 28 novembre 2000, constituent des exemples de faux en informatique : la falsification et/ou la contrefaçon de cartes de crédit, les faux en matière de contrats numériques (lorsque les données juridiquement pertinentes ne sont plus imprimées sur papier ni signées à la main) ou encore l’utilisation de données fausses. On songe encore à l’inscription de créances fictives ou à la modification de données salariales par un employé dans le logiciel comptable de l’entreprise, ou à la falsification d’une signature électronique…

On relève qu’est punissable « comme s’il était l’auteur du faux » celui qui fait usage des données falsifiées en pleine connaissance de cause (art. 210*bis*, § 2).

A la différence des dispositions relatives aux faux traditionnels (art. 193 et s. C. pén.), le nouvel article 210*bis* ne fait pas de distinction suivant la qualité de l’auteur de l’infraction (fonctionnaires, officiers publics, simples particuliers) ou suivant la nature de l’acte falsifié (acte public, acte authentique, acte commercial ou acte privé). Cette différence de régime a été critiquée par le Conseil d’Etat sur la base du principe d’égalité, mais le législateur n’a toutefois pas cru bon de revoir sa copie à cet égard, s’exposant ainsi à un recours devant la Cour d’arbitrage.

Par ailleurs, comme n’a pas manqué de le relever le Conseil d’Etat, il ressort du commentaire de l’article 210*bis* que, contrairement au faux en écriture de droit commun, le faux en informatique ne suppose aucune intention frauduleuse dans le chef de son auteur.  Aussi le faux en informatique requerrait-il uniquement comme élément moral  le *dol général* ? La réponse est non car, suite à un amendement déposé *in extremis* au Sénat, l’article 193 du Code pénal (à lire conjointement avec l’art. 210*bis*) est désormais libellé comme suit : « Le faux en écriture, *en informatique* ou dans des dépêches télégraphiques, avec une intention frauduleuse ou à dessin de nuire, sera puni conformément aux articles suivants » (modifié par l’art. 3 de la L. du 28 novembre 2000). Par conséquent, un *dol spécial* est requis pour le faux et l’usage de faux informatique, comme pour le faux en écriture.

Au total, l’infraction sera établie si et seulement si tous ses éléments constitutifs sont réunis, à savoir :

* Il faut qu’il y ait introduction, modification ou effacement de données dans un système informatique ou encore modification de l’utilisation possible de ces données.
* Il est nécessaire que le faux modifie la portée juridique de ces données (un préjudice est traditionnellement exigé comme condition du faux en écriture). Selon l’exposé des motifs, il revient au juge d’apprécier si cette modification a effectivement lieu.
* Le faux doit être commis avec une intention frauduleuse ou à dessein de nuire. Selon certains auteurs, cette exigence devrait mettre à l’abri d’une condamnation celui qui fabrique de fausses cartes de crédit ou de fausses signatures digitales dans un but scientifique (p. ex. pour démontrer la vulnérabilité d’un système) ou pédagogique.

La seule tentative de faux est également punissable (art. 210*bis*, § 3). Enfin, les peines prévues sont doublées en cas de récidive (art. 210*bis*, § 4).

### 2. La fraude informatique

 **Art. 504*quater*. § 1er.** Celui qui cherche à se procurer, pour lui-même ou pour autrui, avec une intention frauduleuse, un avantage économique illégal en introduisant dans un système informatique, en modifiant ou effaçant des données qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation normale des données dans un système informatique, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de vingt-six euros à cent mille euros ou d'une de ces peines seulement.

**§ 2.** La tentative de commettre l'infraction visée au § 1er est punie d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à cinquante mille euros ou d'une de ces peines seulement.

**§ 3.** Les peines prévues par les §§ 1er et 2 sont doublées si une infraction a l'une de ces dispositions est commise dans les cinq ans qui suivent le prononcé d'une condamnation pour une de ces infractions ou pour une des infractions visées aux articles 210*bis*, 259*bis*, 314*bis* ou au titre IX*bis.*

L’incrimination de fraude informatique vise celui qui cherche à se procurer, pour lui-même ou pour autrui, un avantage économique illégal, par le biais d’une manipulation illicite de données sous forme informatique.

L’élément matériel de l’infraction peut être caractérisé comme suit :

1. l’introduction, la modification ou l’effacement de données informatiques ou la modification de l’utilisation normale de ces données (il n’est pas requis que ces données aient été falsifiées);
2. procurant à l’auteur ou à autrui un avantage économique illégal.

A la différence de l’escroquerie (art. 496 C. pén.), il n’est pas ici question de manipulation directement destinée à tromper la confiance d’une personne pour obtenir la remise d’un bien ; il faut, mais il suffit, que l’avantage économique obtenu à la faveur de l’infraction présente un caractère frauduleux (avantage patrimonial obtenu).

 En ce qui concerne l’élément moral, l’infraction requiert la preuve d’une intention frauduleuse d’obtenir sans droit, par des agissements illicites et/ou des moyens irréguliers, un bénéfice économique, pour soi-même ou pour autrui.

Selon les travaux préparatoires, la fraude informatique peut viser l’utilisation d’une carte de crédit volée pour retirer de l’argent d’un distributeur automatique, le dépassement illicite du crédit octroyé par sa propre carte de crédit, l’introduction d’instructions de programmation permettant d’obtenir à la suite de certaines transactions d’autres résultats en vue d’un avantage financier illicite, ou le détournement à des fins lucratives de fichiers ou de programmes informatiques confiés dans un but spécifique, ou encore les manipulations effectuées par un employé de banque sur les comptes des clients.

La tentative de fraude est également punie (art. 504*quater*, § 2). En cas de récidive, les peines prévues sont doublées (art. 504*quater*, § 3).

La définition de la fraude informatique apparaît particulièrement large. A juste titre, le législateur a été guidé par le souci d’adopter un texte suffisamment large et ouvert, qui puisse résister à l’évolution galopante – faut-il le dire ? – des technologies de l’information. Toute la difficulté est de définir l’infraction avec une précision néanmoins suffisante pour satisfaire au principe de prévisibilité essentiel en droit pénal. Réel défi que celui de parvenir à concilier avec bonheur ces contraintes apparemment contradictoires. L’effet sans doute inattendu du compromis adopté est que certains actes devenus banals sur les réseaux peuvent désormais ressortir à la prévention de fraude. A titre d’illustration, certains auteurs citent le cas – fréquent sur les réseaux – de l’inscription de *cookies* (dits permanents) sur le disque dur de l’ordinateur de l’usager du Web, spécialement lorsqu’ils servent surtout à dresser le profil précis de l’usager à des fins de marketing direct, et ce, en violation de la législation relative à la protection des données à caractère personnel.

### 3. L’accès non autorisé à un système

 **Art. 550*bis*. § 1er.** Celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient, est puni d'un emprisonnement de trois mois à un an et d'une amende de vingt-six euros à vingt-cinq mille euros ou d'une de ces peines seulement.

Si l'infraction visée à l'alinéa 1er, est commise avec une intention frauduleuse, la peine d'emprisonnement est de six mois à deux ans.

**§ 2.** Celui qui, avec une intention frauduleuse ou dans le but de nuire, outrepasse son pouvoir d'accès à un système informatique, est puni d'un emprisonnement de six mois à deux ans et d'une amende de vingt-six euros à vingt-cinq mille euros ou d’une de ces peines seulement.

**§ 3.** Celui qui se trouve dans une des situations visées aux §§ 1er et 2 et qui :
1° soit reprend, de quelque manière que ce soit, les données stockées, traitées ou transmises par le système informatique;

2° soit fait un usage quelconque d'un système informatique appartenant à un tiers ou se sert du système informatique pour accéder au système informatique d'un tiers;

3° soit cause un dommage quelconque, même non intentionnellement, au système informatique ou aux données qui sont stockées traitées ou transmises par ce système ou au système informatique d'un tiers ou aux données qui sont stockées, traitées ou transmises par ce système;

est puni d'un emprisonnement de un à trois ans et d'une amende de vingt-six euros belges à cinquante mille euros ou d'une de ces peines seulement.

**§ 4.** La tentative de commettre une des infractions visées aux §§ 1er et 2 est punie des mêmes peines.

**§ 5.** Celui qui, indûment, possède, produit, vend, obtient en vue de son utilisation, importe, diffuse ou met à disposition sous une autre forme, un quelconque dispositif, y compris des données informatiques, principalement conçu ou adapté pour permettre la commission des infractions prévues aux §§ 1er à 4, est puni d’un emprisonnement de six mois à trois ans et d’une amende de vingt-six euros à cent mille euros ou d’une de ces peines seulement.

**§ 6.** Celui qui ordonne la commission d'une des infractions visées aux §§ 1er à 5 ou qui y incite, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de cent euros à deux cent mille euros ou d'une de ces peines seulement.

**§ 7.** Celui qui, sachant que des données ont été obtenues par la commission d'une des infractions visées aux §§ 1er à 3, les détient, les révèle à une autre personne ou les divulgue, ou fait un usage quelconque des données ainsi obtenues, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à cent mille euros ou d'une de ces peines seulement.

**§ 8.** Les peines prévues par les §§ 1er à 7 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans qui suivent le prononcé d'une condamnation pour une de ces infractions ou pour une des infractions visées aux articles 210*bis*, 259*bis*, 314*bis*, 504*quater* ou 550*ter*.

Le paragraphe 1er du nouvel article 550*bis* réprime l’accès non autorisé à un système informatique ou le fait de s’y maintenir (*hacking* externe), tandis que son paragraphe 2 vise celui qui, avec une intention frauduleuse ou dans le but de nuire, outrepasse son pouvoir d’accès à un système informatique (*hacking* interne). On remarquera que l’élément moral requis diffère dans les deux hypothèses. Un dol spécial est exigé dans le seul cas de *hacking* réalisé depuis l’intérieur de l’entreprise. En revanche, un dol général suffit pour la prévention de hacking externe; si l’infraction est commise avec une intention frauduleuse, la peine s’en trouve seulement aggravée. Dans son avis, le Conseil d’Etat avait pris soin de relever qu’en cas de *hacking* externe, la simple curiosité devient punissable, alors que tel n’est pas le cas hors contexte informatique.

La tentative de commettre les infractions visées à l’article 550*bis*, §§ 1 ou 2 est punie des mêmes peines que l’infraction elle-même (§ 4).

Les cas de *hacking* externe sont bien connus à la faveur de quelques affaires retentissantes relayées par la grande presse. L’élément de maintien dans le système informatique est présent dès l’instant où l’intrus s’y “promène” un certain temps, et ce, quand bien même l’accès au système n’aurait pas été commis de manière illicite (l’effraction n’est pas une condition légale de l’infraction). C’est dire le caractère large – trop large ? – de la nouvelle incrimination. Comme l’a noté le Conseil d’Etat, citant Pol Glineur, cela revient à ériger en infraction l’accès non désiré à un agenda électronique alors que l’accès non désiré à un agenda “papier”, tout aussi confidentiel, demeure impuni. Il est pourtant douteux que la différence objective de support des données supposées confidentielles justifie la différence de traitement au plan pénal, alors que, dans les deux cas, l’atteinte à la confidentialité est pareillement condamnable.

Suite à cet avis critique du Conseil d’Etat, un amendement déposé au Sénat prévoyait l’exigence d’un dol spécial, mais cet amendement a été rejeté par le Gouvernement qui a préféré revenir au texte initial du projet de loi, justifiant son point de vue comme suit : « Il est en effet inacceptable que le hacking intentionnel, mais sans dol spécial, ne soit pas punissable. Cela ouvrirait la voie à toutes sortes d’abus, qui mettraient en danger la sécurité des systèmes informatiques ». La volonté du législateur est clairement de rendre punissable le simple accès non autorisé à un système informatique en vue, par exemple, de tester un système de sécurité.

En revanche, en cas d’introduction illicite dans un système informatique par des utilisateurs jouissant d’un certain pouvoir d’accès (*hacking* interne), un dol spécial est requis. L’outrepassement du pouvoir d’autorisation accordé n’est punissable que si le sujet indélicat (ex. l’employé trop curieux qui va lire des dossiers confidentiels dont il n’est pas censé pouvoir prendre connaissance) est animé d’une intention particulière comme l’appât du gain illicite ou la malveillance. Selon l’exposé des motifs, le simple fait d’entrer illicitement dans des parties du système doit être abordé par le biais de mécanismes moins radicaux (sanctions internes, législation du travail, droit civil...). Cette approche nous apparaît pertinente, et l’on se demande pourquoi elle n’a pas été adoptée également en matière de *hacking* externe.

En son paragraphe 3, l’article 550*bis* prévoit des circonstances aggravantes et un alourdissement de la peine lorsque celui qui accède sans autorisation à un système informatique, tant depuis l’extérieur que de l’intérieur, adopte l’un des comportements suivants :

* reprendre, de quelque manière que ce soit, les données stockées, traitées ou transmises par le système informatique (est ainsi visé, par exemple, le vol de secrets d’entreprise dans le cadre de l’espionnage industriel); ou
* faire un usage quelconque d'un système informatique appartenant à un tiers ou se servir du système informatique pour accéder au système informatique d'un tiers (par exemple, l’utilisation de capacité ou de temps ordinateur, entraînant une limitation temporaire des possibilités d’autres utilisateurs); ou
* causer un dommage quelconque, même non intentionnellement, au système informatique ou aux données qui sont stockées, traitées ou transmises par ce système ou au système informatique d'un tiers ou aux données qui sont stockées, traitées ou transmises par ce système.

L’article 550*bis*, § 5, tel que modifié par la loi du 15 mai 2006, réprime les actes préparatoires, plus précisément la possession, la production, la vente, l’obtention en vue de son utilisation, l’importation, la diffusion ou la mise à disposition sous une autre forme d’un quelconque dispositif, y compris des données informatiques, principalement conçu ou adapté pour commettre un *hacking*. En clair, sont visés les *hackertools*, ces outils logiciels susceptibles de faciliter la commission de faits de *hacking* (en permettant de craquer des sécurités d’accès, de neutraliser des dispositifs de protection d’œuvres couvertes par des droits intellectuels... notamment au départ d’un ordinateur connecté à distance). Ainsi, celui qui élabore, détient ou délivre des dispositifs destinés à faciliter le piratage est lui-même punissable. Cela concerne la publication d’instructions de *hacking*, la conception ou mise à disposition de programmes soumettant des combinaisons de mots de passe, le trafic de codes d’accès, de numéros d’utilisation pour des logiciels ou de mots de passe….

Un dol spécial était requis pour cette infraction avant la modification introduite par la loi du 15 mai 2006. La suppression des mots « avec une intention frauduleuse ou dans le but de nuire » n’entraîne pas condamnation sans nuance des *hackertools* : encore faut-il rapporter la preuve d’un dol général.

Sont également punissables celui qui commandite ou encourage l’infraction (§ 6) et celui qui recèle, divulgue ou fait un usage quelconque des données obtenues suite à la commission de faits de *hacking* (§ 7).

Toutes les peines prévues par l’article 550*bis* sont doublées en cas de récidive (§ 8).

### 4. Le sabotage informatique

**Art. 550*ter*. § 1er.** Celui qui, sachant qu’il n’y est pas autorisé, directement ou indirectement, introduit dans un système informatique, modifie ou efface des données, ou qui modifie par tout moyen technologique l'utilisation normale de données dans un système informatique, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à vingt-cinq mille euros ou d'une de ces peines seulement.

Si l’infraction visée à l’alinéa 1er est commise avec une intention frauduleuse ou dans le but de nuire, la peine d’emprisonnement est de six mois à cinq ans.

**§ 2.** Celui qui, suite à la commission d'une infraction visée au § 1er, cause un dommage à des données dans le système informatique concerné ou dans tout autre système informatique, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de vingt-six euros à septante-cinq mille euros ou d'une de ces peines seulement.

**§ 3.** Celui qui, suite à la commission d'une infraction visée au § 1er, empêche, totalement ou partiellement, le fonctionnement correct du système informatique concerné ou de tout autre système informatique, est puni d'un emprisonnement de un an à cinq ans et d'une amende de vingt-six euros à cent mille euros ou d'une de ces peines seulement.

**§ 4.** Celui qui, avec une intention frauduleuse ou dans le but de nuire, conçoit, met à disposition, diffuse ou commercialise des données stockées, traitées ou transmises par un système informatique, alors qu'il sait que ces données peuvent être utilisées pour causer un dommage à des données ou empêcher, totalement ou partiellement le fonctionnement correct d'un système informatique, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à cent mille euros ou d'une de ces peines seulement.

**§ 5.** Les peines prévues par les §§ 1er à 4 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans qui suivent le prononcé d'une condamnation pour une de ces infractions ou pour une des infractions visées aux articles 210*bis*, 259*bis*, 314*bis*, 504*quater* ou 550*bis*."

**§ 6.** La tentative de commettre l’infraction visée au § 1er est punie des mêmes peines.

Le sabotage informatique vise des actes de destruction tels que la destruction de fichiers ou le fait de rendre inutilisable un système, ou encore la conception et/ou la diffusion de virus.

La destruction de matériel informatique tombe certes sous le coup des incriminations de droit commun prévues par les articles 523 et 559 du Code pénal visant, respectivement, la destruction d’une machine appartenant à autrui et la destruction de propriétés mobilières, soit d’objets tangibles. En revanche, la destruction de données informatiques n’est pas directement punissable au titre des préventions de droit commun. D’où l’incrimination de l’article550*ter*, récemment modifié par la loi du 15 mai 2006.

Contrairement au *hacking*, le commanditaire d’un sabotage n’est pas spécifiquement sanctionné.

Les paragraphes 2 et 3 prévoient des circonstances aggravantes et un alourdissement des peines lorsque le sabotage cause un dommage effectif à des données (§ 2) ou entrave totalement ou partiellement le bon fonctionnement du système informatique concerné (§ 3). A cet égard, on songe au *spamming* ou au *mailbombing* (saturer un serveur d’information ou une messagerie électronique par des envois répétés…).

Est également puni « celui qui, avec une intention frauduleuse ou dans le but de nuire, conçoit, met à disposition, diffuse ou commercialise des données stockées, traitées ou transmises par un système informatique, alors qu'il sait que ces données peuvent être utilisées pour causer un dommage à des données ou empêcher, totalement ou partiellement le fonctionnement correct d'un système informatique » (§ 4). Cette disposition vise spécifiquement à réprimer les actes préparatoires, tels que la conception, la mise à disposition ou la diffusion de virus ou de programmes permettant de créer pareils virus.

Cette infraction requiert un double élément moral : outre l’intention frauduleuse, il faut que l’auteur soit conscient que les données conçues et diffusées sont susceptibles d’endommager des données ou d’entraver l’utilisation d’un système informatique. Par conséquent, l’usager qui propage un virus à son insu (ayant lui-même reçu un virus avec son cortège de vicissitudes : carnet d’adresses infecté, apparition de nouveaux fichiers... et envoi non voulu d’e-mails à divers correspondants... non sélectionnés...) n’est pas punissable.

Enfin, en cas de récidive, les peines prévues sont doublées (§ 5).

Désormais, la tentative est incriminée (§ 6, introduit par la loi du 15 mai 2006) et punie des mêmes peines que le sabotage lui-même. Cette adaptation de la loi belge vise à la mettre en conformité avec la Convention cybercriminalité du Conseil de l’Europe.

**II. L’adaptation de la procédure pénale à la lutte contre la cybercriminalité**

Outre la création de nouvelles infractions devant permettre de combattre efficacement les différentes formes de criminalité dans le cyberespace, le législateur du 28 novembre 2000 a entendu résoudre les problèmes de procédure particuliers posés par la cybercriminalité. A cet égard, il est permis d’épingler, entre autres difficultés pratiques suscitées par la poursuite des infractions et de leurs auteurs sur le *net*,

1° l’inadéquation des procédures judiciaires à la lutte contre la criminalité dans l’environnement numérique (*quid* des concepts reçus de *saisie* et de *perquisition* appliqués à des données immatérielles ?);

2° l’anonymat sous le couvert duquel œuvrent souvent les cybercriminels et la fugacité des traces laissées par eux;

3° la dimension internationale de la cybercriminalité, qui invite à un renforcement des mécanismes de coopération internationale;

4° les besoins accrus en matière d’interception des télécommunications et de conservation des données transmises, ce qui ne va pas sans entraîner des risques inédits en termes de protection des droits de l’homme et de la vie privée; etc.

Pour faire face à ces défis, le législateur n’a pas résisté, comme nous le verrons, à une certaine tentation sécuritaire, au risque de faire entorse à divers principes constitutionnels garantissant les libertés fondamentales des citoyens. Nous aurons l’occasion d’illustrer cette appréciation, ça et là, au cours de notre examen des diverses modifications apportées à nos règles de procédure pénale.

### 1. La saisie de données informatiques

**Art. 39*bis*. § 1er.** Sans préjudice des dispositions spécifiques de cet article, les règles de ce code relatives à la saisie, y compris l'article 28*sexies*, sont applicables aux mesures consistant à copier, rendre inaccessibles et retirer des données stockées dans un système informatique.

**§ 2.** Lorsque le procureur du Roi découvre dans un système informatique des données stockées qui sont utiles pour les mêmes finalités que celles prévues pour la saisie, mais que la saisie du support n'est néanmoins pas souhaitable, ces données, de même que les données nécessaires pour les comprendre, sont copiées sur des supports qui appartiennent à l'autorité. En cas d'urgence ou pour des raisons techniques, il peut être fait usage de supports qui sont disponibles pour des personnes autorisées à utiliser le système informatique.

**§ 3.** Il utilise en outre les moyens techniques appropriés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité.

 Si les données forment l'objet de l'infraction ou ont été produites par l'infraction et si elles sont contraires à l'ordre public ou aux bonnes mœurs ou constituent un danger pour l'intégrité des systèmes informatiques ou pour des données stockées, traitées ou transmises par le biais de tels systèmes, le procureur du Roi utilise tous les moyens techniques appropriés pour rendre ces données inaccessibles. Il peut cependant, sauf dans le cas prévu à l'alinéa précédent, autoriser l'usage ultérieur de l'ensemble ou d'une partie de ces données, lorsque cela ne présente pas de danger pour l'exercice des poursuites.

**§ 4.** Lorsque la mesure prévue au § 2 n'est pas possible, pour des raisons techniques ou à cause du volume des données, le procureur du Roi utilise les moyens techniques appropriés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité.

**§ 5.** Le procureur du Roi informe le responsable du système informatique de la recherche effectuée dans le système informatique et lui communique un résumé des données qui ont été copiées, rendues inaccessibles ou retirées.
**§ 6.** Le procureur du Roi utilise les moyens techniques appropriés pour garantir l'intégrité et la confidentialité de ces données.

Des moyens techniques appropriés sont utilisés pour leur conservation au greffe.

La même règle s'applique, lorsque des données qui sont stockées, traitées ou transmises dans un système informatique sont saisies avec leur support, conformément aux articles précédents.

Le Code d’instruction criminelle n’autorisant pas la saisie de données immatérielles (cf. art. 35 et s.), les autorités policières et judiciaires n’avaient d’autres possibilités que de saisir, dans le cadre de perquisitions, les disques durs ou le matériel informatique des entreprises ou personnes physiques soupçonnées de piratage, d’accès irréguliers à des systèmes informatiques, d’actes de contrefaçon ou d’autres délits encore.

Pareilles mesures étaient ressenties comme particulièrement lourdes et désagréables, tant pour les chargés de la perquisition que pour les « victimes » de celle-ci, et fort préjudiciables (la privation soudaine des principaux outils de travail pouvant parfois entraîner des dommages irréversibles). Elles apparaissaient, en outre, souvent disproportionnées.

Pour faire bonne mesure, il arrivait généralement que seules étaient saisies les données stockées sur un support électronique (disques durs ou supports mobiles).

Désormais, l’article 39*bis* (nouveau) du Code d’instruction criminelle autorise la copie des données, ainsi que le fait de rendre inaccessibles et de retirer des données stockées dans un système informatique (lire le § 1er). On s’avise que ces mesures n’aboutissent pas à soustraire les données à leur détenteur si bien que l’on a affaire à un mode nouveau de saisie… « sans dépossession ». Les §§ 2 à 6 explicitent les modalités de « saisie » des données.

Lorsque la saisie des supports n’est pas souhaitable, les données seront copiées, en principe, sur des supports appartenant à l’autorité. En cas d’urgence ou pour des raisons techniques (le volume des données excède les capacités de stockage des supports amenés par l’autorité), elles pourront néanmoins être copiées sur des supports de l’entreprise perquisitionnée. La copie concerne aussi « les données nécessaires pour les comprendre », c’est-à-dire les outils permettant de les lire (logiciels ayant servi à la création des données) ou de restituer en clair des données chiffrées (clés de décryptage) (§ 2).

En outre, le procureur du Roi peut empêcher l’accès aux données ayant fait l’objet de copies (notamment par le biais de leur chiffrement), de manière à priver le saisi de la maîtrise des « biens saisis » et à éviter que l’original des données copiées soit altéré et, ainsi, ne puisse plus servir à titre probatoire (§ 3, alinéa 1). Comme le précise le § 4, ce blocage d’accès peut remplacer la copie des données lorsque celle-ci s’avère impossible (raisons techniques ou volume des données).

L’alinéa 2 du paragraphe 3 semble redondant par rapport à l’alinéa 1er. Apparemment il s’en distingue en ce qu’il permet l’*élimination* de certains types de données (contraires à l’ordre public ou aux bonnes mœurs : images pédopornographiques, virus…) après qu’une copie en ait été réalisée pour les besoins de la justice. En revanche, tous les autres types de données ne peuvent être détruits dans le cadre des mesures d’instruction, en dehors d’un jugement rendu au fond.

Lorsque les données « saisies » se trouvent dans le système informatique d’un tiers, le responsable du système doit être informé de la recherche effectuée et un résumé des données copiées, rendues inaccessibles ou retirées, doit lui être communiqué (§ 5).

### 2. La recherche sur les réseaux

**Art. 88*ter*. § 1er.** Lorsque le juge d'instruction ordonne une recherche dans un système informatique ou une partie de celui-ci, cette recherche peut être étendue vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée :

 - si cette extension est nécessaire pour la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche, et

 - si d'autres mesures seraient disproportionnées, ou s'il existe un risque que, sans cette extension, des éléments de preuve soient perdus.

**§ 2.** L'extension de la recherche dans un système informatique ne peut pas excéder les systèmes informatiques ou les parties de tels systèmes auxquels les personnes autorisées à utiliser le système informatique qui fait l'objet de la mesure ont spécifiquement accès.

**§ 3.** En ce qui concerne les données recueillies par l'extension de la recherche dans un système informatique, qui sont utiles pour les mêmes finalités que celles prévues pour la saisie, les règles prévues à l'article 39*bis* s'appliquent. Le juge d'instruction informe le responsable du système informatique, sauf si son identité ou son adresse ne peuvent être raisonnablement retrouvées.

Lorsqu'il s'avère que ces données ne se trouvent pas sur le territoire du Royaume, elles peuvent seulement être copiées. Dans ce cas, le juge d'instruction, par l'intermédiaire du ministère public, communique sans délai cette information au ministère de la Justice, qui en informe les autorités compétentes de l'état concerné, si celui-ci peut raisonnablement être déterminé.

**§ 4.** L'article 89*bis* est applicable à l'extension de la recherche dans un système informatique.

Les mandats de perquisition délivrés par le juge d’instruction visent normalement un lieu précis (domicile privé, siège de l’entreprise…) où il espère trouver des indices de l’infraction supposée. Or, pour constater des infractions commises dans un environnement de réseaux, la recherche doit souvent s’étendre à des informations et des systèmes localisés en dehors du lieu de perquisition. L’article 88*ter* permet, en cas de recherche dans un système informatique, d’étendre cette recherche vers un système informatique situé en un autre lieu que celui où la recherche est effectuée :

* si cette extension est nécessaire pour la manifestation de la vérité à l’égard de l’infraction qui fait l’objet de la recherche, et
* si d’autres mesures seraient disproportionnées, ou s’il existe un risque que, sans cette extension, des éléments de preuve soient perdus.

Les deux conditions cumulatives figurant dans l’art. 88*ter*, § 1er, ainsi que les autres restrictions prévues au texte (lire aussi le § 2), visent à contenir dans des limites raisonnables l’ampleur géographique de l’extension de la recherche. A défaut, interconnexions aidant, c’est tout le *world wide web* qui pourrait y passer… Il n’est donc pas question que les enquêteurs puissent accéder à des systèmes étrangers au système visé par le mandat de perquisition.

Les données recueillies par l’extension de la recherche pourront être saisies conformément aux règles prévues à l’article 39*bis*. Néanmoins, si ces données se trouvent dans un système localisé à l’étranger, elles peuvent seulement être copiées (§ 3). Cette sorte de perquisition transfrontalière sur réseau, menée par les enquêteurs sans l’autorisation préalable des autorités compétentes de l’Etat concerné, semble constituer une violation de la souveraineté et du droit international, comme l’a relevé le Conseil d’Etat, à la suite du Conseil de l’Europe. Manifestement, le législateur belge a agi avec précipitation à cet égard, alors que la solution préconisée est sur le point de s’imposer au niveau adéquat, c’est-à-dire, naturellement, au niveau international.

### 3. Les obligations d’information et de coopération

**Art. 88*quater*. § 1er.** Le juge d'instruction ou un officier de police judiciaire auxiliaire du procureur du Roi délégué par lui, peut ordonner aux personnes dont il présume qu'elles ont une connaissance particulière du système informatique qui fait l'objet de la recherche ou des services qui permettent de protéger ou de crypter des données qui sont stockées, traitées ou transmises par un système informatique, de fournir des informations sur le fonctionnement de ce système et sur la manière d'y accéder ou d'accéder aux données qui sont stockées, traitées ou transmises par un tel système, dans une forme compréhensible. Le juge d'instruction mentionne les circonstances propres à l'affaire justifiant la mesure dans une ordonnance motivée qu'il transmet au procureur du Roi.
**§ 2.** Le juge d'instruction peut ordonner à toute personne appropriée de mettre en fonctionnement elle-même le système informatique ou, selon le cas, de rechercher, rendre accessibles, copier, rendre inaccessibles ou retirer les données pertinentes qui sont stockées, traitées ou transmises par ce système, dans la forme qu'il aura demandée. Ces personnes sont tenues d'y donner suite, dans la mesure de leurs moyens.

L'ordonnance visée à l'alinéa 1er, ne peut être prise à l'égard de l'inculpé et à l'égard des personnes visées à l'article 156.

**§ 3.** Celui qui refuse de fournir la collaboration ordonnée aux §§ 1er et 2 ou qui fait obstacle à la recherche dans le système informatique, est puni d'un emprisonnement de six mois à un an et d'une amende de vingt-six euros à vingt mille euros ou d'une de ces peines seulement.

**§ 4.** Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

**§ 5.** L'Etat est civilement responsable pour le dommage causé de façon non intentionnelle par les personnes requises à un système informatique ou aux données qui sont stockées, traitées ou transmises par un tel système.

Dans leur recherche en vue d’établir les infractions informatiques et d’en démasquer les auteurs, les enquêteurs peuvent se heurter aux cryptosystèmes utilisés par les pirates et autres cybercriminels. A quoi bon disposer de copies des données suspectes ou étendre leur recherche vers d’autres systèmes si les données saisies et copiées ne peuvent être déchiffrées. C’est le revers des mesures de sécurité tant recommandées pour garantir l’intégrité et la confidentialité des communications électroniques. Il importe donc que les autorités chargées d’enquêtes puissent requérir la collaboration des personnes disposant des clés d’accès aux systèmes informatiques et aux données y stockées.

En bref, le nouvel article 88*quater*, § 1er, permet au juge d'instruction ou à un officier de police judiciaire auxiliaire du procureur du Roi d’ordonner aux personnes dont il estime qu'elles ont une connaissance particulière du système informatique qui fait l'objet de la recherche de fournir des informations sur le fonctionnement du système et sur la manière d'y accéder ou d'accéder aux données (en ce compris la façon de faire sauter des protections, ou de déchiffrer des informations codées…).

En complément, le § 2 prévoit que « le juge d'instruction peut ordonner à toute personne appropriée de mettre en fonctionnement elle-même le système informatique ou, selon le cas, de rechercher, rendre accessibles, copier, rendre inaccessibles ou retirer les données pertinentes qui sont stockées, traitées ou transmises par ce système, dans la forme qu'il aura demandée. Ces personnes sont tenues d'y donner suite, dans la mesure de leurs moyens ».

Toutefois cet ordre ne peut être donné à l’inculpé ou à ses proches. Cette dernière solution est conforme au principe du « droit au silence » autorisant une personne à se taire si elle est accusée d’une infraction, et à ne pas fournir une information qui serait susceptible de l’incriminer. Ce « droit au silence » est inscrit dans le Pacte international relatif aux droits civils et politiques de New York. Il est reconnu par la Cour européenne des droits de l’homme et érigé en principe général de droit par la Cour de cassation.

Le refus de collaboration est sanctionné pénalement (§ 3).

Peuvent être ainsi tenus de prêter leur coopération non seulement le responsable du système informatique concerné, ses principaux utilisateurs, le gestionnaire du réseau, le concepteur ou le fournisseur du logiciel de décryptage, des tiers de confiance (prestataires de services de certification…), mais aussi – pourquoi pas ? – des experts en sécurité informatique, spécialistes de la cryptographie qui maîtriseraient le cryptosystème sécurisant les données litigieuses…

On s’interroge sur la possibilité dont disposerait le juge d’instruction, sur pied de l’article 88*ter*, d’exiger la remise des clés de cryptage. Pareille obligation viserait les concepteurs des clés, leur fournisseur ou les tiers de confiance. La prudence s’impose quant à systématiser cette remise des clés de chiffrement. En effet, on ne saurait oublier que ces clés donnent accès à quantité de données, dont certaines seulement sont pertinentes au regard de l’instruction en cours. Or le juge d’instruction ne jouit pas nécessairement d’un accès légitime à toutes ces autres données. Par ailleurs, les autorités policières ou judiciaires ne se voient imposer aucune obligation spécifique en termes de sécurité et de protection des clés qui leur sont confiées, avec les risques de vol ou de détournement entraînés par cette lacune.

### 4. L’interception des communications

[**Art.**](http://www.juridat.be/cgi_loi/loi_a1.pl?cn=1808111730&language=fr&caller=list&la=F&fromtab=loi&tri=dd+AS+RANK&rech=1&numero=1&sql=(text+contains+(''))#Art.90bis#Art.90bis) **90*ter*. § 1er.** Lorsque les nécessités de l'instruction l’exigent, le juge d’instruction peut, à titre exceptionnel, écouter, prendre connaissance et enregistrer, pendant leur transmission, des communications ou des télécommunications privées, s’il existe des indices sérieux que le fait dont il est saisi constitue une infraction visée par l’une des dispositions énumérées au § 2, et si les autres moyens d’investigation ne suffisent pas à la manifestation de la vérité.

En vue de permettre l’écoute, la prise de connaissance ou l’enregistrement direct de communications ou télécommunications privées à l’aide de moyens techniques, le juge d'instruction peut également à l’insu ou sans le consentement de l’occupant, du propriétaire ou de ses ayants droit, ordonner la pénétration, à tout moment, dans un domicile ou dans un lieu privé.

La mesure de surveillance ne peut être ordonnée qu’à l’égard soit de personnes soupçonnées, sur la base d’indices précis, d’avoir commis l’infraction, soit à l’égard des moyens de communication ou de télécommunication régulièrement utilisés par un suspect, soit à l’égard des lieux présumés fréquentés par celui-ci. Elle peut l’être également à l’égard de personnes présumées, sur la base de faits précis, être en communication régulière avec un suspect.

Aux termes des articles 90*ter* et 90*quater*, § 4, du Code d’instruction criminelle, le juge d'instruction peut ordonner aux opérateurs de services de télécommunications ou de services de cryptage de collaborer à l’interception de toute communication numérique. Sont ainsi autorisées de véritables « écoutes électroniques » dès lors qu’il s’agit d’intercepter des données numériques en cours de transmission. Ne relève pas de ce genre d’interceptions la consultation d’un e-mail ou d’un SMS après réception.

Ces mesures – attentatoires à la vie privée – doivent être appliquées dans le respect du principe de proportionnalité. C’est pourquoi elles ne peuvent être ordonnées que dans le cadre d’enquêtes relatives aux infractions reprises à l’article 90*ter*, § 2, du Code d’instruction criminelle.

### 5. Repérage (art. 88*bis* C.I.Cr.) et identification (art. 46*bis* C.I.Cr.) sur base des données de télécommunications

La loi du 28 novembre 2000 (art. 14) a modifié l’article 109*ter* de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques autonomes.

Désormais, il est imposé aux opérateurs de réseaux et aux fournisseurs de services de télécommunications une obligation d’enregistrement et de conservation des données d’appel et des données d’identification d’utilisateurs de services de télécommunications. Cette obligation est instaurée « en vue de l’investigation et de la poursuite d’infractions pénales ». Le « délai [de conservation des données], qui ne peut jamais être inférieur à 12 mois, ainsi que les données d’appel et d’identification doivent encore être déterminés par arrêté royal délibéré en Conseil des ministres, après avis de la Commission pour la protection de la vie privée ».

On observera l’imprécision – ou mieux : le caractère particulièrement large – des termes utilisés pour définir les débiteurs de l’obligation de conservation. Ainsi, les opérateurs de réseaux téléphoniques ou mobilophoniques, les fournisseurs d’accès à l’internet, de courriers électroniques, de services *chat*, de forums de discussion, etc. devront conserver toutes les données relatives aux appels, communications et connexions… L’obligation de conservation est de surcroît permanente, et non liée à une instruction en cours, c’est-à-dire à une recherche précise et déterminée d’infractions (à la différence de l’obligation de coopération évoquée précédemment). Avec la Commission de la protection de la vie privée, on doute que le principe constitutionnel fondamental de proportionnalité soit ici respecté.

Comme précisé plus haut, les cas et types de données concernés par l’obligation de conservation doivent encore être déterminés par arrêté royal. A cet égard, la loi s’oppose au principe constitutionnel de légalité selon lequel il appartient au législateur seul d’apporter des restrictions au droit à la vie privée. En outre, la loi ne définit pas ce qu’elle entend par « données ». Or les données d’appel et d’identification peuvent inclure, notamment, les adresses IP des ordinateurs émetteurs et récepteurs des communications, la liste de tous les sites consultés et de tous les e-mails échangés, ainsi que leur contenu… Nombre de ces données constituent indubitablement des données à caractère personnel, éventuellement sensibles, protégées par la loi belge relative à la vie privée, dont les principes ne semblent pas clairement applicables à cette obligation de conservation.

Telles sont quelques-uns des reproches que l’on peut adresser à un texte de loi qui, répondant à un réflexe sécuritaire compréhensible, met à mal certaines libertés fondamentales et, singulièrement, le droit au respect de la vie privée.