

# *Fiche de l'AWT*

## *La criminalité informatique*

Face à la menace que représente la criminalité informatique, la Belgique dispose d'une législation spécifique réprimant la cyberdélinquance

Créée le 16/02/01  
Modifiée le 20/06/02

# 1. Présentation de la fiche

---

*Face à la menace que représente la criminalité informatique, la Belgique dispose d'une législation spécifique réprimant la cyberdélinquance*

**La qualification juridique du concept de criminalité informatique représente un exercice délicat tant la nature et l'importance des actes délictueux commis peuvent être variables.** L'accroissement significatif du nombre d'affaires concernant de tels actes au cours de ces dix dernières années est lié au développement exponentiel des capacités d'échange et de stockage de données numériques, notamment au travers d'infrastructures ouvertes telles que l'Internet.

**Cette fiche présente les enjeux et les principales définitions de la criminalité informatique, notamment au travers du cadre législatif adopté en Belgique.**

## 1.1. Fichiers à télécharger

---

- **Loi "criminalité informatique"** (format .PDF)  
Loi du 28 novembre 2000 relative à la criminalité informatique (moniteur belge du 3 février 2001)

## 1.2. Sites Web en rapport avec cette fiche

---

- **Droit et technologie**  
Portail créé et mis à jour par une équipe de juristes et d'ingénieurs, il présente et analyse l'actualité du droit des TIC en Belgique et à l'étranger (actualités, dossiers, textes législatifs, etc.)  
<http://www.droit-technologie.org>
- **Direction générale de la société de l'information**  
Elle joue un rôle capital dans la mise en oeuvre de la vision définie par les chefs d'État européens à Lisbonne en 2000, à savoir faire de l'Europe, d'ici à 2010, l'économie la plus compétitive et la plus dynamique du monde, se caractérisant par une croissance durable, créant davantage d'emplois plus qualifiés et garantissant une plus grande cohésion sociale  
[http://europa.eu.int/comm/dgs/information\\_society/index\\_fr.htm](http://europa.eu.int/comm/dgs/information_society/index_fr.htm)
- **Juriscom**  
Revue juridique spécialisée dans le droit des technologies de l'information qui publie régulièrement les contributions (articles, mémoires, débats...) de nombreux juristes, universitaires ou professionnels, etc.  
<http://www.juriscom.net>
- **Direction générale de la justice et des affaires intérieures**  
Son rôle est de maintenir et développer l'union européenne en tant qu'espace de liberté, de sécurité et de justice, comme cela est prévu par le traité d'Amsterdam  
[http://europa.eu.int/comm/dgs/justice\\_home/index\\_fr.htm](http://europa.eu.int/comm/dgs/justice_home/index_fr.htm)
- **Forum européen sur la cyber-criminalité**  
Ce forum fournit une plateforme pour la discussion et la coopération entre les organes nationaux compétents en matière de cyber-criminalité, les ISP (Internet Service Provider), les opérateurs de télécommunications, les organismes ayant en charge le respect de la vie privée, les associations de protection des consommateurs, etc.  
<http://cybercrime-forum.jrc.it>

## 2. Qualification juridique

*Qualification juridique et cadre législatif de la criminalité informatique*

**Afin de préciser la notion de criminalité informatique, il convient de distinguer deux situations différentes:**

- **le support informatique n'est qu'un instrument facilitant l'accomplissement d'un délit conventionnel** (contrefaçon, détournement de fonds, escroquerie, détention et recel de contenus illicites, dénigrement, diffamation via des services en ligne, etc.),
- **le support informatique est l'objet même du délit** (vol d'informations, accès non autorisés aux données ou aux systèmes à des fins délictueuses, etc.).

**C'est seulement dans cette seconde hypothèse que l'on parlera véritablement de cybercriminalité.**



**Face à la globalisation de cette délinquance informatique, les frontières étatiques représentent un handicap considérable pour assurer une identification claire et une répression efficace des responsables. Chaque pays dispose d'une législation différente visant à réprimer de tels actes.**

En Europe, la Suède fait figure de pionnier, puisqu'elle a été le premier pays à adopter, en 1973, une législation spécifique réprimant l'acquisition non autorisée de données informatiques. D'autres Etats membres de l'UE, comme les Pays-Bas ou la France avec la loi Godfrain ont à leur tour adopté de telles législations début des années 90.

**En Belgique**, en l'absence de texte spécifique, la répression des actes de cyberdélinquance relevait précédemment d'une jurisprudence instable car celle-ci devait s'appuyer sur des textes disparates formant un ensemble peu cohérent. Les insuffisances de ces textes ne permettaient pas aux Cours et Tribunaux d'adapter les incriminations traditionnelles, telles que le faux ou encore le vol, aux actes criminels ayant pour cible des technologies nouvelles. Par ailleurs, la nature même des actes de cyberdélinquance n'incite généralement pas les victimes à faire publiquement état des faiblesses de leurs systèmes informatiques. Il était donc indispensable d'adopter une législation pour mettre un terme à cette insécurité juridique peu compatible avec les exigences de la société de l'information.

## 2.1. Le cadre législatif

---

**Le 8 novembre 2001 a vu l'adoption par 30 états de la Convention du Conseil de l'Europe (COE) sur la cybercriminalité. Des Etats tels que les Etats-Unis, le Canada, le Japon et l'Afrique du Sud ont également signé ce traité. La Convention a été ouverte à la signature le 23 novembre 2001. Elle entrera en vigueur dès que cinq Etats, dont au moins trois membres du Conseil de l'Europe, l'auront ratifié.** Lors de son élaboration, ce texte a fait l'objet de nombreuses critiques de la part de la des organisations de défense des libertés qui le jugeait par trop attentatoire à la vie privée des citoyens. Tenant compte de ces observations, le texte finalement adopté est nettement moins répressif. **La convention de novembre 2001 vise à:**

- harmoniser les éléments des infractions ayant trait au droit pénal matériel national et les dispositions connexes en matière de cybercriminalité,
- fournir au droit pénal procédural national les pouvoirs nécessaires à l'instruction et à la poursuite d'infractions de ce type ainsi que d'autres infractions commises au moyen d'un système informatique ou dans le cadre desquelles des preuves existent sous forme électronique,
- mettre en place un régime rapide et efficace de coopération internationale.

**Le texte classe les infractions commises sur les réseaux électroniques en quatre catégories distinctes:**

- les infractions à l'encontre de la confidentialité, de l'intégrité, de la disponibilité des données et des systèmes,
- les infractions informatiques: falsification et fraudes informatiques,
- les infractions concernant le contenu: acte de production, diffusion, possession de pornographie enfantine, propagation de thèses racistes et xénophobes,
- les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes.

**La Convention du COE précise également certains points essentiels en matière de procédure dans les affaires de cybercriminalité.** En effet, lorsque des preuves existent sous forme électronique, il convient d'établir des règles permettant d'assurer la sauvegarde de celles-ci pour les besoins de l'enquête. Cette exigence concerne plus particulièrement:

- la conservation rapide de données stockées dans un système informatique,
- la conservation et la divulgation rapide de données relatives au trafic,
- les injonctions de produire,
- les perquisitions et les saisies de données informatiques stockées,
- la collecte en temps réel des données relatives au trafic,
- l'interception de données relatives au contenu.

Enfin, le texte du COE aborde également les problèmes de compétence juridictionnelle ainsi que la question essentielle de la coopération entre les autorités policières et judiciaires.

**De son côté, la Belgique a adopté dès l'automne 2000 une loi relative à la criminalité informatique** (loi du 28 novembre 2000, moniteur belge du 3 février 2001). Cette loi permet l'incrimination de quatre nouvelles formes de délits:

- le faux et l'usage de faux en informatique,
- la fraude informatique et la tentative de fraude,
- le hacking et la tentative de hacking,
- le sabotage informatique.

## 3. Les quatre formes de délits visés par la loi belge

*Faux et usages de faux. La fraude et la tentative de fraude. L'accès non autorisé (hacking). Le sabotage de données*

**Les nouvelles dispositions de l'article 210 bis § 1 concernent:** "les personnes qui commettent 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. De la même manière que le faux, la tentative de faux est tout autant punissable".

### 3.1. Faux et usages de faux



**La confection de faux contrats électroniques ou de fausses cartes de paiement ou de crédit** constituent des exemples de faux en informatique.

**Contrairement au faux en écriture en droit commun, le faux en informatique ne requiert aucune intention particulière.** Le faux en informatique ou sa tentative est punissable d'un emprisonnement de 6 mois à 5 ans et d'une amende de 26 francs à 100000 francs.

### 3.2. La fraude et la tentative de fraude

**La fraude informatique ou sa tentative seront souvent associées au faux en informatique.** Cette incrimination vise à sanctionner celui qui intentionnellement se procure frauduleusement, pour lui-même ou pour autrui, un avantage de nature patrimoniale en introduisant, modifiant ou en effaçant des données stockées, traitées ou transmises dans un système informatique.



**Parmi les actes susceptibles de tomber sous le coup d'une telle infraction, on peut notamment citer:**

- l'utilisation d'une carte de paiement ou de crédit volée,
- l'introduction d'instructions de programmation visant à en retirer un avantage financier illicite,
- le détournement de fichiers ou de programmes à des fins lucratives.

**Les peines encourues sont identiques à celles prévues pour le faux et la tentative de faux en informatique.** Des dispositions aggravantes sont également prévues en cas de récidive.

### 3.3. L'accès non autorisé (hacking)

---

**Le hacking peut être défini comme le fait d'accéder de façon illicite à des données ou à tout ou partie d'un système informatique ou de s'y maintenir.** Les peines encourues pour hacking ou sa tentative de délit vont d'un emprisonnement compris entre 3 mois à un an et/ou 26 francs à 25000 francs d'amende.

**Le texte vise à la fois les hypothèses d'accès non autorisé réalisé par des tiers ainsi que celles mises en œuvre en interne.** Dans ce dernier cas, les peines encourues sont alourdies car l'intention de nuire est caractérisée (de 6 mois à 2 ans d'emprisonnement).

L'accès non autorisé à des données ou à des systèmes informatiques concerne donc à la fois le fait de prendre connaissance de données pour soi-même ou pour autrui, mais aussi le fait de s'emparer de données. Le commanditaire d'actes de hacking encoure des peines alourdies compte tenu de sa position (jusqu'à 5 ans d'emprisonnement et /ou 200000 francs d'amende) De la même manière, le fait de recourir intentionnellement à des techniques affectant les capacités des systèmes informatiques (hackertools) est également constitutif de circonstances aggravantes.

**Le recel de données obtenues par ce moyen est également réprimé.** Des dispositions aggravantes sont prévues en cas de récidive.

### 3.4. Le sabotage de données

---

**Cette incrimination n'est pas nouvelle en soi, notre droit réprimait en effet déjà le sabotage du matériel, mais elle est dorénavant étendue au sabotage de données.** La loi sanctionne celui qui introduit, modifie ou efface des données dans l'intention de nuire.



**Le texte établit une gradation des peines en fonction des conséquences du dommage. Plusieurs cas de figure sont prévus:**

- sabotage de données,
- sabotage de données causant un dommage,
- sabotage d'un système informatique,
- toute manipulation dans une intention frauduleuse permettant d'élaborer un sabotage. Cette dernière hypothèse vise plus spécialement la création et la diffusion de virus informatiques.

Si des dispositions particulières ont également été prises en cas de récidive, le commanditaire d'un acte de sabotage ne semble en revanche pas avoir été visé par la loi.

## 4. Limites des méthodes d'investigation et réponses de la loi belge

*Les limites classiques des méthodes d'investigation. Les réponses de la loi belge à ces obstacles. Obligations de collaboration des utilisateurs et intermédiaires techniques. Pouvoirs accrus en faveur du juge d'instruction*

### 4.1. Les limites classiques des méthodes d'investigation

**La lutte contre la criminalité informatique se heurte à 3 obstacles majeurs:**

- **la localisation et l'identification des délinquants:** il faut pouvoir accéder aux fichiers log des ISP et opérateurs tout en respectant les principes fondamentaux de respect de la vie privée et de droit à l'anonymat;
- **la préservation des éléments de preuve:** cette exigence impose quant à elle d'être en mesure de contrôler les données stockées sur les terminaux informatiques de l'utilisateur final et/ou celles éventuellement stockées pour son compte par un prestataire extérieur;
- **le stockage des données:** la nature transnationale de l'Internet multiplie les possibilités de stockage en différents lieux géographiques. Dès lors, il sera souvent nécessaire, dans le cadre d'investigations visant à identifier les responsabilités de procéder à des recherches de données stockées à l'étranger. Cette situation impose la mise en place d'une coopération internationale efficace qui est susceptible de remettre en cause la souveraineté des Etats.

### 4.2. Les réponses de la loi belge à ces obstacles

Afin de surmonter en partie ces difficultés, la nouvelle loi modifie la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, ainsi que plusieurs dispositions du Code d'instruction criminelle. **Ces modifications prévoient notamment l'instauration de nouvelles obligations et l'octroi de pouvoirs plus étendus pour lutter plus efficacement contre la cybercriminalité.** Ces nouvelles mesures s'organisent donc autour des axes suivants:

- des obligations de collaboration des utilisateurs et des intermédiaires techniques,
- des pouvoirs accrus en faveur du juge d'instruction.

### 4.3. Obligations de collaboration des utilisateurs et intermédiaires techniques

**Le texte impose dorénavant aux opérateurs de télécommunications et aux ISP d'enregistrer et de conserver, pendant un délai (qui ne peut être inférieur à un an) les données d'appel et d'identification des utilisateurs de leurs services de télécommunications (origine, destination, lieu, durée).** En cas de non-respect de ces obligations, la loi prévoit une peine d'emprisonnement pouvant aller de 3 à 6 mois et/ou une amende comprise entre 26 francs et 20 000 francs. Un arrêté royal viendra déterminer les différentes modalités de ces nouvelles exigences.

Par ailleurs, **afin d'être en mesure de déchiffrer les données cryptées,** la loi prévoit la collaboration des personnes qui sont présumées avoir une connaissance particulière du système informatique concerné. Celles-ci sont alors tenues de s'exécuter dans la mesure de leurs moyens. Le refus de collaboration est passible d'une peine d'emprisonnement de 6 mois à un an et/ou d'une amende comprise entre 26 francs et 20000 francs.

## 4.4. Pouvoirs accrus en faveur du juge d'instruction

---

**Le juge d'instruction se voit reconnaître des prérogatives étendues en matière de lutte contre la criminalité informatique.** Désormais, lorsqu'il ordonne une recherche dans un système informatique ou une partie de celui-ci, il peut élargir cette investigation vers un système se trouvant dans un lieu différent de celui où la recherche est effectuée y compris à l'étranger.

**Plusieurs conditions doivent être réunies pour mettre en œuvre cette mesure d'extension:**

- elle doit être nécessaire,
- la mise en place d'autres mesures plus habituelles serait disproportionnée,
- elle ne peut être mise en œuvre que dans le cadre d'une affaire déjà en phase d'instruction,
- elle ne peut pas dépasser les niveaux d'accès préalablement définis.



**Lorsque les données concernées se trouvent hors de Belgique, celles-ci ne peuvent être que copiées.** L'état étranger sur le territoire duquel se trouvent ces données doit alors être informé par le ministère de la justice. Cette dernière disposition ne règle en aucun cas les questions relatives à la nécessité d'une coopération internationale en matière de cybercriminalité. Ces questions sont actuellement débattues au sein du Conseil de l'Europe. Une convention internationale pourrait enfin voir prochainement le jour. Parallèlement à ces travaux, l'UE vient de jeter, dans le cadre de l'initiative e-Europe 2002, les bases d'un plan d'action destiné à renforcer la lutte contre la cybercriminalité.

**Enfin, la nouvelle loi règle les questions de procédures relatives à la saisie des données informatiques** ainsi que les modalités de leur conservation notamment en ce qui concerne le respect de l'intégrité et de la confidentialité des informations qui y sont contenues.

---



© **Agence Wallonne des Télécommunications**  
Avenue de Stassart 16 à 5000 Namur - Belgium  
[www.awt.be](http://www.awt.be) - [info@awt.be](mailto:info@awt.be)