Sanctions juridiques

Atteintes à un système d'information

- Accès et maintien dans un système d'information
- Atteinte au fonctionnement d'un système d'information
- Atteinte aux données d'un système d'information
- Diffusion d'un logiciel d'intrusion

Atteintes à un système d'information

Accès et maintien dans un système d'information

2 Ans d'emprisonnement et 30000

€ d'amende pour le fait d'accèder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données

3 ans et 45000 € s'il y a, involontairement suppression, modification des données ou altération du système

Pour constituer ces infractions, il faut 3 conditions:

- présence d'un système de traitement automatisé de données
- une réalisation effective (élément matériel)
- une intention frauduleuse de la réaliser (élément moral)

Et si le système n'était pas sécurisé?

Jurisprudence floue, mais pour le moment, condamnable

Atteintes à un système d'information

Atteinte au fonctionnement d' un système d'information	5 ans de prison et 75000 € d'amende
	Entraver le fonctionnement du système: la finalité est de bloquer le système
	Fausser le fonctionnement du système: faire fonctionner le système de manière erronée

Atteintes à un système d'information

Atteinte aux données d'un système d'information	5 ans de prison et 75000€ d'amende
	Fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient
	L'accès frauduleux n'est pas nécessaire et une personne ayant un droit d'accès, non animé de la volonté de nuire, peut être condamnée sur ce chef dès lors que les opérations effectuées sur les données sont fautives.

Atteintes à un système d'information

Diffusion d'un logiciel d'intrusion

Article 323-3-1 du codé pénal, créé par la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN), punit le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues

Par exception, cet article prévoit la détention de ce type de logiceiles pour des motis légitimes

Cet exception permet donc aux spécialistes de l'anti-intrusion d 'analyser, de créer et d'éprouver ces dispositifs à des fins de sécurisation des systèmes d'information, sous réserve de prendre certaines précautions évoquées dans le présent chapitre.

Atteintes aux traitements de données à caractère personnel

- Tout traitement de données à caractère personnel doit être déclaré à la CNIL, autorité administrative indépendante créée par la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (dite « loi Informatique et libertés ») modifiée.

Atteintes aux traitements de données à caractère personnel

- Notion de données à caractère personnel:
  - Constituée par toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui est propre.

Atteintes aux traitements de données à caractère personnel

- Les catégories de données à caractère personnel:
  - Etat-civil, Identité, données d'identification;
  - Vie personnelle (habitudes de vie, situation familiale…)
  - Vie professionnelle (CV, scolarité…)
  - Informations économiques et financières (revenus, situation fiscale…)
  - Données de connexion (IP…)
  - Données de localisation (données GPS, GSM…)

Atteintes aux traitements de données à caractère personnel

- Les données dites sensibles dont traitement prohibé, autorisé que par exception
  - Numéro de sécurité social
  - Infractions, condamnations
  - Opinions philosophiques, politiques, religieuses, données de santé…
- Le cas de l'adresse IP
- Le cas « Acadomia »

Atteintes aux traitements de données à caractère personnel

- Collecte illicite de données à caractère personnel
  - 5 ans de prison, 300 000 € le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite.
- Divulgation illicite de données à caractère personnel
  - Divulgation sans autorisation de l'intéressé
  - Communiquées à un tiers qui n'a pas la qualité de les recevoir
  - 5 ans de prison, 300 000 € d'amende

Atteintes aux traitements de données à caractère personnel

- Obligation de sécurité du responsable de traitement
  - Le responsable du traitement de données à caractère personnel visé par une attaque est défini comme étant celui qui détermine les finalités et les moyens de ce traitement
  - Obligation de sécurité du responsable de traitement
  - Doit s'assurer de la traçabilité des actions sur le système d'information (qui a accès, à quoi et pourquoi? Qui a fait quoi? …)
  - Doit établir des contrats avec prestataires et sous-traitants
  - Guide CNIL de la sécurité

Atteintes aux traitements de données à caractère personnel

- L'obligation de moyen devient une obligation de résultat:
  - Depuis fin août 2011, obligation pour les responsables de traitement de déclarer tout incident sur les données à caractère personnel à la CNIL et … aux personnes physiques concernées.

Infractions classiques applicables à l'informatique

- Usurpation d'identité
  - Création d'un délit d'usurpation sur internet pour répondre aux dérives sur les réseaux sociaux et actes d'ingénierie sociale
  - Par la loi d'orientation et de programmation pour la performance de la sécurité intérieur (LOPPSI 2)

Infractions classiques applicables à l'informatique

- La messagerie
  - « le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers , ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45000€ d'amende »
  - correspondance privée:
    - si le message est exclusivement destiné à une ou plusieurs personnes, physique ou morale.
  - Email inclus
  - Contenu Facebook est-il une correspondance privée?