Sécurité et fraude en informatique: Aspects juridiques

présenté par :

- **Amina Dik**

Ingénieur en chef, Docteur en droit privé

OWASP AppSec Morocco & Africa 2018

- **Casablanca, Le 16 -11 - 2018**

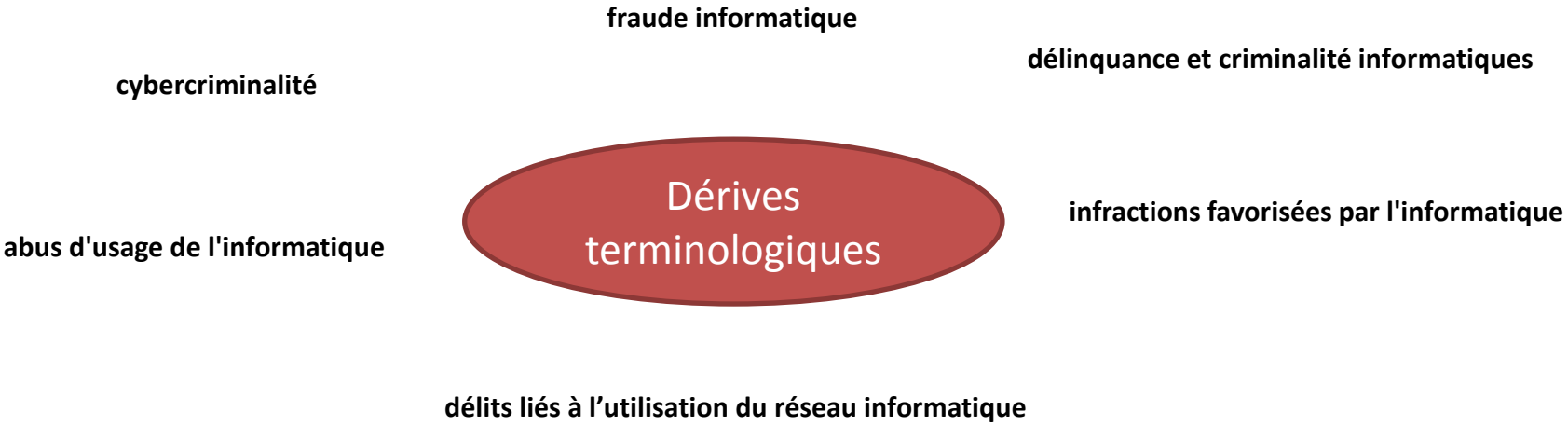
PLAN

Introduction

- L'économie mondiale = économie numérique, basée sur l'échange d'informations dotées d'une valeur économique.

- Or cet échange emprunte comme moyen de circulation les réseaux informatiques. Ce qui rend les informations et les réseaux des cibles d'agressions connues sous le terme de **Fraude informatique**.

- La fraude informatique n'est pas défini légalement, mais l'est par la doctrine et la jurisprudence.
- Il faut la différencier des autres termes ayant trait à la criminalité informatique.



Cybercriminalité (I) = *L'ensemble des infractions commises* ***à l'aide*** *ou* ***contre*** *un système informatique connecté au réseau de télécommunication.*

La fraude informatique(II) = *Toute action illicite perpétrée à l'aide d'opération électronique* ***contre*** *la sécurité d'un système informatique ou de données qu'il contient, quelque soit le but visé.*

I

II

Objet de délit

- Les atteintes, usage et accès indu aux S.I
- La création ou diffusion de programmes
- Les infractions ayant trait à la protection des données personnelles
- Les infractions à la législation sur la cryptologie

Moyen du délit

- atteintes pénales aux libertés individuelles
- atteintes pénales aux biens (Faux, vol, escroquerie, abus de confiance)
- atteintes pénales à l'ordre public (Actes de trahison, espionnage, terrorisme)
- atteintes pénales au code de la propriété intellectuelle (contrefaçon - piratage)

Mesures réprimant la fraude des systèmes d’informations

Les articles du code pénal incriminant les infractions informatiques se trouvent dans le chapitre 10 sous le titre « *de l'atteinte aux systèmes de traitement automatisé des données* ».

La loi 07.03 ⇨ les articles 607-3 à 607- 11 du Code pénal

Accès frauduleux et maintien dans un système d'information

Accès frauduleux dans un système d'information

- L'article 607-3 du Code pénal stipule : « *Le fait d'accéder, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni* ***d'un mois à trois mois d'emprisonnement*** *et de* ***2 000 à 10 000 dirhams*** *d'amende ou de l'une de ces deux peines seulement* » .

Constats (Accès frauduleux dans un système d'information)

- connexion illégale
- appel d'un programme
- exploration du contenu
- lorsqu'un salarié ayant quitté son emploi pénètre dans le système de son ancien employeur
- le maître d'ouvrage qui après réalisation de son œuvre et conclusion du contrat, ayant gardé les mots de passe, accède au système
- de l'employé qui outrepasse ses pouvoirs en s'introduisant dans des parties interdites et confidentielles du système.

Maintien frauduleux dans un système d'information

- Le second alinéa de l''article 607-3 du Code pénal stipule: «*Est passible de la même peine toute personne qui* ***se maintient dans tout ou partie d'un système*** *de traitement automatisé de données auquel elle a accédé par erreur et alors qu'elle n'en a pas le droit* » .

Constats (maintien frauduleux dans un système d'information)

- Le législateur réprime le maintien frauduleux dans les systèmes informatiques, et ce même s'il résulte d'un accès régulier antérieur.
- l'auteur qui effectue une opération différente que celle initialement prévue
- effectue une opération en dépassant le temps de connexion autorisé
- cas du fraudeur habilité à accéder à une partie du système qui, ayant eu frauduleusement accès à une partie non autorisée de ce système, s'y maintient en connaissance de cause
- cas du fraudeur qui ayant eu par hasard accès à un système fermé, s'y maintient volontairement tout en sachant qu'il n'en a pas droit.

Constats (maintien frauduleux dans un système d'information)

- la volonté de l'accès ou du maintien à elle seule est punie, l'intention de nuire n'étant pas nécessaire

- les intrusions avec dommages sont plus sévèrement sanctionnées du moment que la peine est portée au double lorsqu'il en résulte une altération du fonctionnement du système d'information.

Atteintes volontaires au fonctionnement d'un système informatique

Entrave

- A l'instar de l'article 5 de la Convention sur la cybercriminalité, l'art 607-5 du Code Pénal sanctionne le fait d'entraver un système d'information.

- l'art 607-5 du Code Pénal = «*Le fait d'entraver ou de fausser intentionnellement le fonctionnement d'un système de traitement automatisé de données est puni d'un an à trois ans d'emprisonnement et de 10.000 à 200.000 dirhams d'amende ou de l'une de ces deux peines seulement.* »

Entrave

- Elle « *est synonyme de gêne, d'empêchement* », et couvre tous les agissements empêchant le fonctionnement partiel ou total, logiciel ou matériel du système

- Elle englobe le plus grand nombre de comportements issus **des mécanismes viraux** allant du « *changement de mot de passe d'un ordinateur ou d'un réseau dans le but de le rendre inutilisable par l'administrateur réseau* », au lancement d'une attaque par «*déni de service*» ou *l'arrêt* même du système.

Exemples:

- la destruction des fichiers systèmes garantissant le bon fonctionnement dudit système
- L'encombrement de sa mémoire suite à une propagation des virus.
- programmer l'envoi d'un grand nombre de messages, de simuler de multiples connexions sur un serveur, ayant pour effet le ralentissement de sa capacité de traitement.
- L'entrave «interne» d'une personne ayant droit à l'accès et au maintien = un directeur technique ayant changé les codes d'accès du système informatique de l'entreprise, refuse de les communiquer aux autres et arrête totalement le système. (En France)
- Un employé licencié d'une entreprise ayant gardé les mots de passe du portail de l'entreprise, avait en premier lieu bloqué les mails dudit portail, et ensuite supprimé le siteweb de l'entreprise. (Au Maroc)

Faussement d'un système

- Faussement = il s'agit des actes provocant **altération, défiguration, dénaturation** du système, ou tout simplement « *lui [faisant] produire un résultat non attendu* » .

- C'est toute altération du système le conduisant à produire un résultat différent de ce qu'il aurait dû être.

- L'utilisation des logiciels susceptibles de perturber le système d'information ou fausser son fonctionnement normal: virus , vers ou bombes logiques .

Faussement d'un système

- Aux termes de l'article 607-10 du code pénal, le législateur marocain réprime aussi les actions correspondant à ***la fabrication, fourniture, ou détention*** des ***programmes viraux***, ainsi que les ***dispositifs*** permettant la commission des infractions informatiques.

- même si ***le programmeur d'un virus*** ne l'utilise pas en personne pour s'introduire dans un système informatique, il est sanctionné au regard des dispositions de cet article ***pour le fait de fabrication de programme malicieux***, une fois le préjudice subi

Mesures réprimant la fraude relative aux données

Constats (Atteintes à l'intégrité des données)

- Atteintes contre les données (contenues dans un système)
  - altérations involontaires: 607 – 3 (al.3)
  - altérations volontaires: 607 – 6

- 607 – 6 = «*Le fait d'introduire frauduleusement des données dans un système de traitement automatisé des données ou de détériorer ou de supprimer ou de modifier frauduleusement les données qu'il contient, leur mode de traitement ou de transmission».*

Constats (Atteintes à l'intégrité des données)

- L'altération de données est incriminée sans se préoccuper ni de la réalité ou non de ces données, ni de leur quantité, ni même de l'état du système (connecté ou autre).

- Au Maroc, elle est sanctionnée sans que cette altération **ait des conséquences**. Aux USA, il faut qu'il ait **préjudice causé à autrui.**

- Exemples:
  - manipulations effectuées par un employé de banque modifiant les comptes des clients
  - manipulations effectuées par un fonctionnaire modifiant la pension des retraités.

Constats (Atteintes à l'intégrité des données)

- L'infraction se manifeste quand l'une des actions suivantes est réalisée:
  - ✓ Suppression ou modification de données
  - ✓ Suppression ou modification du mode de traitement ou de transmission

- La suppression des données informatiques= tout acte qui rend les données inaccessibles à leur propriétaire ou exploitant

- la modification = toute atteinte à la confidentialité, l'intégrité et la disponibilité de l'information, telles:
  - la modification de l'apparence des sites Web
  - la modification des rapports financiers stockés électroniquement

Constats (Atteintes à l'intégrité des données)

- Falsification en informatique = altération du contenu d'un document informatisé. (art 607-7 C.P)
- Pour certains, elle ne devrait pas être traité différemment que le faux en écriture (art 351 du CP), mais d'autres ont contesté cet avis.
- La loi exige qu'elle soit de nature à causer préjudice à autrui, c.à.d que le document informatique doit avoir **une portée juridique**.
- l'usage intentionnel et en pleine connaissance de cause du tel document falsifié est incriminé, et la même peine est infligée

Constats (Atteintes relatives aux données à caractère personnel)

- la loi n°09-08 vise à mettre à la disposition du système juridique marocain des mécanismes légaux spécifiques pour garantir la protection effective des données personnelles contre toute collecte ou utilisation frauduleuse.

- Le premier article de la loi 09-08 définit la donnée comme: « *Toute information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, concernant une personne physique identifiée ou identifiable*».

Constats (Atteintes relatives aux données à caractère personnel)

- Données à caractère personnel = des informations qui permettent d'identifier individuellement une personne physique:
  - de *manière directe* (lorsque son nom apparaît dans un fichier par exemple)
  - ou *indirecte* par des informations telles l'adresse IP de son ordinateur, le numéro de téléphone, l'empreinte digitale....

Constats (Atteintes relatives aux données à caractère personnel)

- Le **traitement** qui fait l'objet de la protection des données à caractère personnel = concerne l'ensemble d'opérations portant sur des données à caractère personnel réalisés ou non par le biais de procédés automatisés, tels « *la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction* »

- Cette définition est large, et considère ainsi tout moyen de gestion de données, toute intervention sur un fichier, comme un traitement.

Constats (Atteintes relatives aux données à caractère personnel)

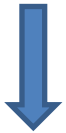
Le traitement est cadré par des principes directeurs:

- droits avant et après traitement
- obligations du responsable du traitement

Principe	Portée
transparence	Découle du droit à l'information / consentement de la personne est nécessaire
légalité	Collecte des informations de manière non déloyale
finalité	Assure que les données sont traitées dans le seul but fixé lors de leur collecte
proportionnalité	Seules sont traitées les données nécessaires au but fixé
conservation	Les données doivent être conservées pendant une durée limitée

Constats (Atteintes relatives aux données à caractère personnel)

- La loi exige de toute personne qui ordonne ou effectue un traitement automatisé de données à caractère personnel de prendre des précautions nécessaires pour préserver **la sécurité** des dites données et empêcher leur **déformation ou endommagement**.



- La demande d'autorisation du traitement = une description générale permettant d'apprécier de façon préliminaire le caractère approprié des mesures prises pour assurer la confidentialité et la sécurité du traitement

Constats (Atteintes relatives aux données à caractère personnel)

- Le manque de sécurité est puni, en vertu de l'article 58 de la loi 09.08, d'un emprisonnement de trois mois à un an et/ou d'une amende de 20.000 à 200.000 DH,

- Le fait de porter ces données, sans autorisation de l'intéressé, à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est considéré comme un délit (art 4) (exemple: les analyses médicales d'un patient)

Constats (Atteintes relatives aux données à caractère personnel)

- Les données « sensibles »
- Certaines données présentent des risques majeurs et sont interdites du traitement
- les transferts de données à caractère personnel vers un pays tiers :

niveau de protection suffisant → autorisés

pas d'un tel niveau de protection → non autorisés

sauf dérogations limitativement énumérées.

L’arsenal organisationnel

L’arsenal organisationnel

Les moyens institutionnels de lutte contre la fraude informatique

Coordination et veille stratégique **CSSSI** **DGSSI** **Ma-Cert**

Contrôle et répression **Direction de police judiciaire** **CNDP**

CSSSI = Comité Stratégique de la Sécurité des Systèmes d’Information

DGSSI = Direction Générale de Sécurité des Systèmes d’Information

CNDP = Commission Nationale de Protection des Données Personnelles

- **CSSSI**: Organe stratégique en charge de la protection de l'information de souveraineté et de garantie de la continuité de fonctionnement des SI des ***infrastructures vitales.***

- **DGSSI**: Organe de coordination de la mise en œuvre des stratégies de Sécurité SI

- **Ma-CERT:** Centres d'alerte et de réaction aux attaques informatiques, destinés aux entreprises et aux administrations publiques.

- **CNDP:** Chargée de vérifier que les traitements des données personnelles sont licites, légaux et ne portent pas atteinte à la vie privée, aux libertés et droits fondamentaux.

- **Direction de police judiciaire:**
  - le *service de lutte contre la criminalité liées aux nouvelles technologies*
  - l'*Unité Analyse des Traces Numériques*
  - *cellule de cybercriminalité au niveau de la Brigade Nationale de la Police Judiciaire*
  - *des laboratoires.*
  - *des points de contact au niveau des services extérieurs de la Police Judiciaire.*

Encadrement juridique de la sécurité informatique

- sécurité informatique = Mise en place de mesures techniques, organisationnelles et juridiques.
- Sur **le plan juridique** =

  Cadrer la sécurité informatique en adoptant des règles imposant la mise en œuvre des mesures de sécurité et d'évaluation de risques, ainsi qu'une politique de publication de faille de sécurité et de fuite d'informations.

  - élaborer des directives internationales ou régionales
  - Adopter de lois dans plusieurs pays
  - Etablir des recommandations par des organismes privés ou publics

Plusieurs projets ont été entamés sur le plan international pour que les solutions techniques apportent des réponses au problèmes juridiques posés par la technique.

1 – Recommandations et lignes directrices des partenaires de la sécurité:

- OCDE
- Résolution 57/239 de l'assemblée générale des nations unies (règles minima de sécurité).
- Résolution 58/199 (réduire au minimum les dégâts et des délais de remise en état en cas d'endommagement ou d'attaque).

2 – Le sommet mondial sur la société de l'information (établir une responsabilisation en matière de sécurité).

3 – L'assemblée mondiale de normalisation des télécommunications (Résolution 50 constitue une feuille de route).

Directive Nationale de la Sécurité des Systèmes d'Information instaurée par la DGSSI

- Il s'agit du premier texte de référence nationale en matière de sécurité des SI
- La DNSSI s'inspire des bonnes pratiques internationales en matière de sécurité des SI
- La DNSSI définit 29 Objectifs de sécurité et 104 règles de sécurité à appliquer
- La DNSSI instruit la définition d'un plan d'action de conformité

Les obligations légales de sécurité

Obligation de sécurité et de confidentialité des données

Le manquement à l'obligation de sécurité

- Sur le plan juridique, **la directive 95/46 du 24 octobre 1995** énumère la sécurité technique parmi les principes de la protection.
- Elle a par sa finalité et son contenu servi de support aux institutions européennes et de modèle aux législations nationales (USA, France, Tunisie).
- Au Maroc, la **loi 09.08** protège l'intégrité et le bon fonctionnement et usage des données à caractère personnel et leur garantit une protection analogue à celles des biens corporels.
- Elle prévoit **l'obligation de prudence et de sécurité** des données. Faute de quoi, le responsable **peut se faire sanctionner** pour le délit de manquement à l'obligation de sécurité, en vertu de l'article 58 de ladite loi.

Le manquement à l'obligation de sécurité

- sur le plan des communications électroniques, l'obligation de sécurité émane également de la directive n° 2002/58 du 12 juillet 2002 relative au traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

- Au Maroc, l'obligation de sécurité est imposée par l'art 52 du P.C.N qui contraint les cybercommerçants à publier les informations relatives aux mesures de sécurité et de contrôle mises en œuvre afin de protéger les données à caractère personnel des utilisateurs.

- Le P.CN encourage via son article 53 le recours à des certifications de la qualité des mesures entreprises pour assurer cette sécurité des échanges et des données.

Obligation de notification des failles de sécurité

Obligation de notification des failles de sécurité

- Les entreprises ont fait rarement publier l'incident vu l'impact de cette publication sur leur e-réputation.

- La personne concernée peut porter plainte au titre du délit de manquement à l'obligation de sécurité, mais il lui faut prouver **le non-respect des mesures de sécurité nécessaires** lors de l'incident. Or l'état de la sécurité du système au jour de l'incident peut être revu et les failles corrigées avant que la personne concernée présente sa plainte.

- Pour instaurer un cadre plus protecteur, les entreprises se trouvent contraints à une obligation de notification de failles de sécurité.

Obligation de notification des failles de sécurité

- L'obligation de notification des fuites de données est déjà en vigueur en Allemagne (2009), en Autriche (2010), au Canada, en Australie et dans les États-Unis d'Amérique.

- Au Maroc, la notification des failles de sécurités n'est pas érigée en obligation. La loi 09.08 en vigueur impose seulement certaines obligations concernant la sécurité du traitement et la confidentialité des données.

Obligation de notification des failles de sécurité

- les sanctions du manquement à l'obligation de notification dans le texte français sont l'emprisonnement et une amende.
- Dans le texte belge, il est sanctionné par une amende.
- Le texte luxembourgeois opte pour un avertissement par la Commission nationale pour la protection des données au fournisseur lors d'un premier manquement aux obligations de notification, et une amende en cas de manquement répété.
- Au Maroc, l'article 105 du P.C.N inflige une amende au manquement de notification.

Merci de votre attention