

Première partie

Droit de l'informatique

Table des matières

I	Droit de l'informatique	1
1	L'informatique et les libertés individuelles	3
1.1	Nos libertés individuelles à l'ère technologique	3
1.2	Le protecteur de nos libertés : la CNIL	4
2	La Cyber conflictualité La Cyber Guerre	7
2.1	Notions Cyberspace, Cyber conflictualité	7
2.2	Les types d'attaques	8
2.3	Les conséquences des attaques	8
2.4	La réponse des États	9

Chapitre 1

L'informatique et les libertés individuelles

1.1 Nos libertés individuelles à l'ère technologique

Nos 4 libertés fondamentales :

Notre droit à l'anonymat dans nos déplacements, question

- De la géolocalisation
- De la vidéo protection :
 - Filment : la voie publique et les lieux ouverts au public et sont soumis aux dispositions du code de la sécurité intérieure.
- De la vidéo surveillance :
 - Concernent : lieux non ouverts au public (bureaux ou réserves des magasins) et soumis aux dispositions de la loi « Informatique et Libertés ».
- **Droit à la préservation de notre identité**
- **Droit à la transparence**
- **Droit à la vie privée**
 - La vie privée, en fait il faut pour être précis dire plutôt « le droit à l'intimité de la vie privée » fait partie des droits civils.
vie privée \Rightarrow pas déf pour éviter de limiter la protection aux seules prévisions légales.

Définition biométrie CNIL : La biométrie regroupe l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales. Les données biométriques sont des données à caractère personnel car elles permettent d'identifier une personne.

ex : Amazon Recognition

Pays déployé biométrie \Rightarrow Chine.

1.2 Le protecteur de nos libertés : la CNIL

Commission Nationale de l'Informatique et des Libertés

Créée en **1978**

Mission générale de la CNIL : Veiller à ce que l'info soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

La CNIL est une **Autorité Administrative Indépendante** car :

- statut assure son indépendance vis-à-vis de l'État
- représentée par une personne physique, son président (Isabelle Falque Pierrotin)

Composition de la CNIL : La commission se compose de **18 membres**

Moyens de la CNIL :

- 17 161 536 € de budget en 2017
- 198 agents à fin 2017

Missions de la CNIL :

— Informer

La CNIL informe les personnes droits et obligations. Elle propose au gouvernement mesures de nature à adapter la protection des libertés et de la vie privée à l'évolution des techniques.

Rmq : Pour création E, CNIL met en avant le principe du « **privacy by design** » : prise en compte de la loi Informatique et Libertés et du RGPD dès la conception du produit ou service.

— Recenser les fichiers

La CNIL exerce, pour le compte des citoyens qui souhaitent, l'accès aux fichiers intéressant la sûreté de l'État, la défense et la sécurité publique notamment ceux des Renseignements Généraux et de Police Judiciaire. 2017 : 4039 D d'accès.

— Garantir le droit d'accès

— Contrôler

La CNIL vérifie que la loi est respectée en contrôlant les applications informatiques.

La Commission use de ses pouvoirs de vérification et d'investigation :

- Pour instruire les plaintes
- Pour disposer d'une meilleure connaissance de certains fichiers
- Pour mieux apprécier les conséquences du recours à l'informatique dans certains secteurs

ex : Sanction Google 2014 (Non application du droit à l'oubli)

A la fin 2017 :

- 341 contrôles
- 79 mises en demeure (= ultimatum pour solutionner un problème)
- 14 sanctions

Quelques sanction 2018 :

- Janvier : Darty, 100 000€ (Insuffisance à la sécurisation des données des clients ayant eu recours au SAV en ligne)

— **Réglementer**

La CNIL établit des normes simplifiées pour que les traitements les + courants et les - dangereux pour les libertés fassent l'objet de formalités allégées.

RGPD : 25 mai 2018

RGPD : Règlement G sur la Protection des Données

GDPR : General Data Protection Regulation

But : **unifier les approches de la réglementation des données de tous les États membres**, en veillant à ce que **toutes les lois sur la protection des données soient appliquées de la même manière** dans l'ensemble de ces pays.

OTT : over the top (en contournant le fournisseur d'accès internet, exemple : Netflix)

Marché volatile : variation du cours de la bourse importante

Avant, le **CIL = Correspondant Informatique et Libertés**

Après, le **DPO = Data Protection Officer = délégué à la protection des données**

Depuis 2005, E, établissements publics, associations peuvent désigner un Correspondant Informatique et Libertés.

- Fin 2017 : 18 802

- Nombres de CIL en France fin 2017 : 5107

Avantage principal :

- Allègement des formalités auprès de la CNIL.

Principales caractéristiques du CIL (DPO) :

- Il doit être indépendant : Pas responsable des traitements informatiques

- Il peut assurer d'autres fonctions : Direction juridique, service qualité

- Il doit avoir les qualifications nécessaires
- Il peut s'agir d'une personne interne ou externe à l'organisation
- Il peut être désigné par plusieurs organisations

DPO \Rightarrow super CIL

Pour les entreprises qui ont un CIL, ce dernier est légitime à occuper cette fonction.

DPO \Rightarrow **périmètre plus large.**

« Le CIL arrête la liste des traitements et s'assure de leur conformité. Le DPO va devoir, lui, **savoir évaluer les risques**».

Double culture de la gestion des risques et de la conformité mais aussi des compétences en IT et en sécurité.

Chapitre 2

La Cyber conflictualité | La Cyber Guerre

2.1 Notions Cyberspace, Cyber conflictualité

Cyberspace Selon l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), Le cyberspace est l'espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numérisées. Caractérisé par une approche sédimentaire en trois couches :

- Physique ou Matérielle
Regroupe les appareils d'extrémité (ordinateurs, box de fournisseur d'accès internet, disques durs, carte de crédit, distributeur de billet de banque. . .) ainsi que les infrastructures réseau.
- Logique ou Logicielle
Regroupe les dispositifs de codage et de programmation qu'utilisent les machines.
La pensée humaine est transformée en information via des interfaces homme-machine et des protocoles permettant la communication entre machines au sein d'un réseau, afin qu'elles puissent se transmettre l'information.
- Sémantique, Cognitive ou informationnelle
Regroupent les données ou métadonnées qui sont transportées par le réseau.
Métadonnées \Rightarrow données de masse
Elles peuvent déterminer les goûts et influencer ou favoriser la prise de décision des conso.

Métadonnées : données qui en décrivent d'autres.

Ex : L'auteur, la date de création, la date de modification et la taille du

fichier

Cyberconflit : Echange d'actions qui utilisent des outils cyber ou des agression cyber pour aider chaque partie à obtenir un avantage sur l'autre dans le cadre de la rivalité qui les oppose. Caractéristiques ?

- Les attaques peuvent être l'œuvre d'un Etat, d'une entreprise, de militants, de particuliers et avoir diverses cibles.
- Il s'agit d'une guerre asymétrique :
 - Faibles coûts
 - Accessible par tous
 - Avantage offensif

rmq : l'attaquant est en situation de force car coût de l'attaque \Rightarrow faible alors que se défendre \Rightarrow coup élevé

2.2 Les types d'attaques

Les conflictualités dans le cyber peuvent être caractérisées par une ou plusieurs combinaisons :

- D'actions cyber espionnage de recherches d'informations
- D'actions correspondant à des cyberattaques :
 - D'actions de perturbation
 - De destruction
 - De prise de contrôle à distance de système informatique
 - D'actions de propagande et de manipulation de l'information assimilable à de la perturbation pour modifier l'opinion

2.3 Les conséquences des attaques

Conséquence d'une attaque ?

- Physique pour la population : paralysie des services médicaux, risque accru d'accident de la route suite au défaut de signalisation...
- Psychologiques
- Environnementales : effets sur la maintenance des sites nucléaires, dysfonctionnement des égouts...
- Économiques : pertes industrielles, financières, sociales...
- Politiques : émeutes
- Liées au cumul et à la combinaison des circonstances ci-dessus

2.4 La réponse des États

États Unis

- Le cybercommand
- Annoncée en 2007
- Création effective en 2009
- Organisation d'opérations de simulation d'attaques

France

- L'ANSSI : Agence Nationale de la Sécurité des Système d'Information
⇒ défense
- Créée en juillet 2009
- Missions ?
 - Détecter attaques
 - Prévenir menace
 - Conseiller adm et OIV
 - Informer régulièrement E et grand public
- Force Offensive, mise en œuvre Décembre 2017
- D'ici 2019, 2600 combattants numériques
- 4400 réservistes
- Budget : 250 millions d'€ par an
- Objectif offensif
- Data Dome