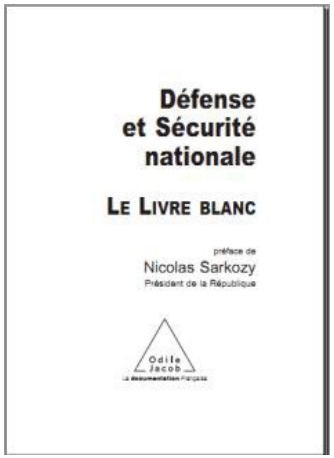
5. Le droit des T.I.C. et l'organisation de la cybersécurité en France

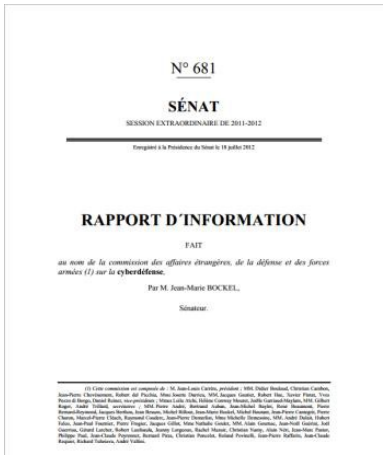
a) L'organisation de la sécurité en France
b) Le contexte juridique
c) Le droits des T.I.C.
d) La lutte contre la cybercriminalité en France
e) En France, Europe et dans le monde : NIS et RGPD

5. Le droit des T.I.C. et l'organisation de la cybersécurité en France

a. L'organisation de la sécurité en France

Cyberdéfense : un véritable enjeu de sécurité nationale





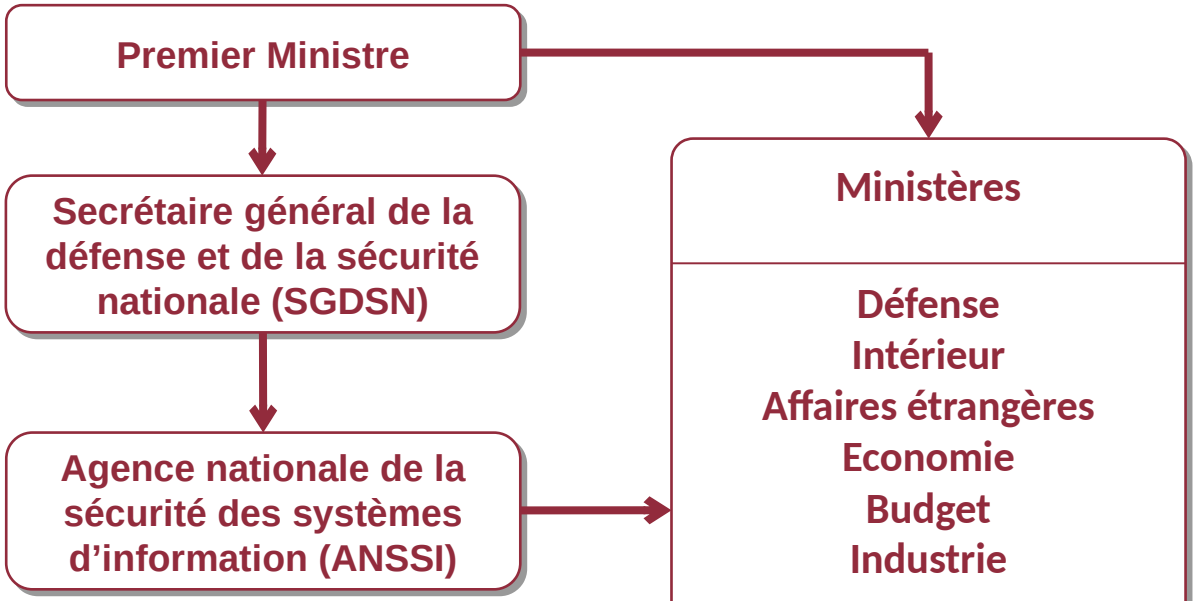
« **Les cyberattaques**, *parce qu'elles n'ont pas, jusqu'à présent, causé la mort d'hommes, n'ont pas dans l'opinion l'impact d'actes terroristes. Cependant, dès aujourd'hui, et plus encore à l'horizon du Livre blanc, elles constituent* **une menace majeure, à forte probabilité et à fort *impact potentiel*** *» (Chapitre 4, Les priorités stratégiques, livre blanc 2013)*

« Le développement de capacités de cyberdéfense militaire fera l'objet ***d'un effort marqué*** *» (Chapitre 7, Les moyens de la stratégie, , livre blanc 2013)*

5. Le droit des T.I.C. et l'organisation de la cybersécurité en France

a. L'organisation de la sécurité en France

Organisation interministérielle :



Pilotage de la politique nationale en matière de sécurité des systèmes d'information

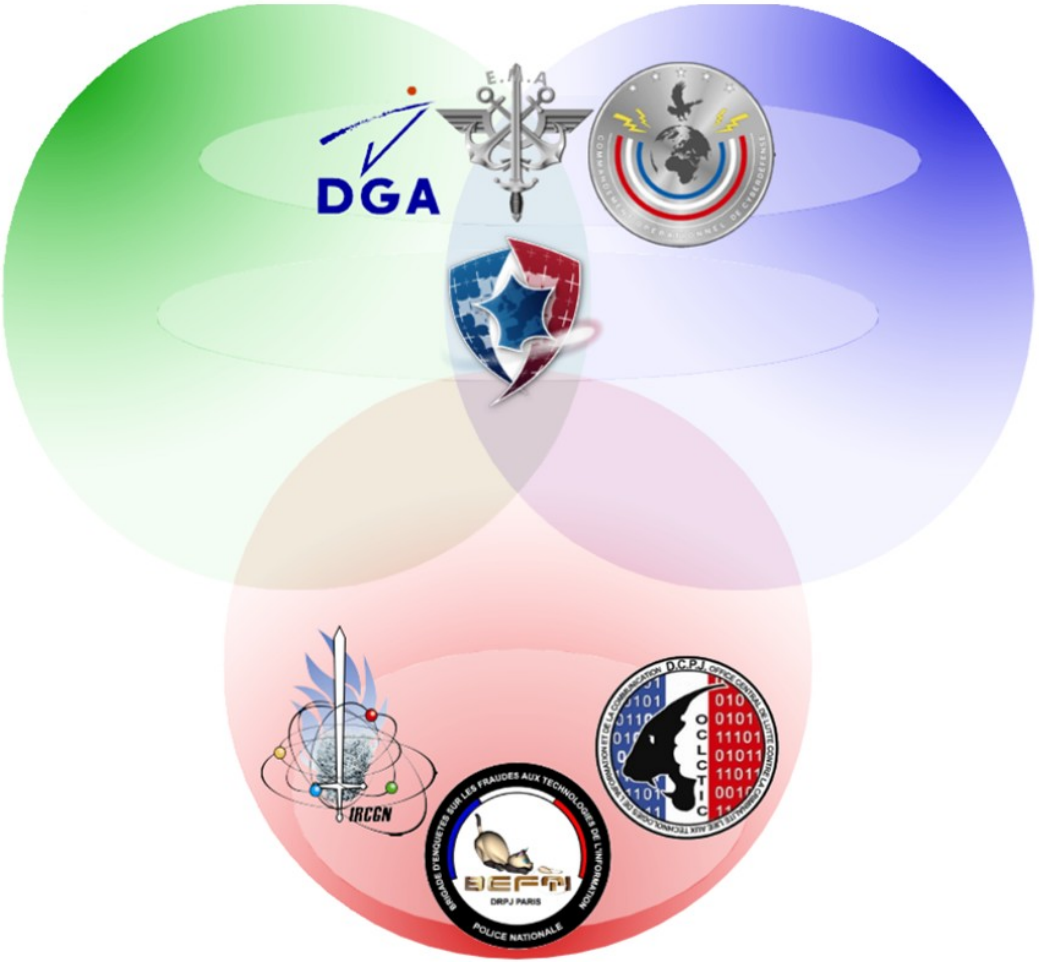
Proposition des règles à appliquer pour la protection des S.I. de l'État.
Vérification de l'application des mesures adoptées
Conseil/soutien Sécurité aux administrations
Information du public
Contribution au développement de Services de confiance
…

Coordination de la préparation des mesures de défense (Vigipirate) et chargés de la sécurité des systèmes d'information

5. Le droit des T.I.C. et l'organisation de la cybersécurité en France

a. L'organisation de la sécurité en France

Cybersécurité = SSI + cyberdéfense + cybercriminalité



- Préfecture de Police (BEFTI)
- Direction Général de l'Armement (DGA)
- Etat-Major des Armées (EMA)
- Gendarmerie Nationale (IRCGN)
- Police Nationale (OCLCTIC)
- Officier Général "Cyber"

5. Le droit des T.I.C. et l'organisation de la cybersécurité en France

b. Le contexte juridique

- Quels domaines doivent être couverts ?

Liberté d'expression

Protection du e-commerce

Propriété intellectuelle

Protection de la vie privée

Protection des entreprises

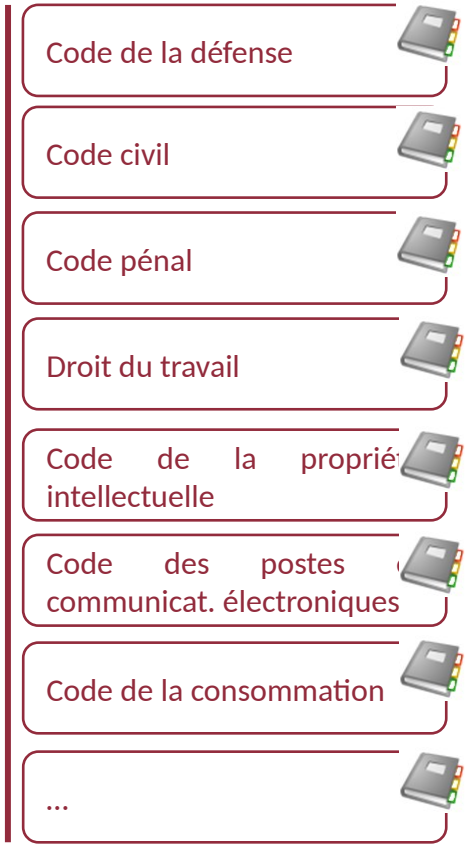
Cybercriminalité

… et bien d'autres…

5. Le droit des T.I.C. et l'organisation de la cybersécurité en France

c. Le droit des T.I.C.

- Un droit non codifié : des dizaines de codes en vigueur
- … et difficile d'accès
  - Au carrefour des autres droits
  - En évolution constante et rapide
  - Issu de textes de toute nature /niveaux
  - Caractérisé par une forte construction jurisprudentielle*
- nécessitant un effort de veille juridique.



(*) La « jurisprudence » est formée de l'ensemble des décisions de justice , « à tous les étages » de l'ordre judiciaire, ce qui donne lieu parfois à des décisions contradictoires, à l'image de l'évolution de la société.

5. La cybersécurité en Europe

Chronologie :

- 20/12/2017 : Création du CERT-UE (coopération lutte cyberattaques et réponse coordonnée)
- 9/4/2019 : Règlement « Cybersecurity Act » qui crée directement :
  - un **cadre de certification à l'échelle de l'UE** (produits, services et processus TIC) sous forme de règles, exigences et procédures,
  - qui permettra la création d'une **agence de l'UE pour la cybersécurité** (modernisation de l'agence de l'UE chargée de la sécurité des réseaux et de l'information -ENISA- en étendant ses compétences et en lui donnant un mandat permanent)
  - et impose des **sanctions aux responsables, soutiens ou impliqués** dans des attaques ou tentatives (y compris états ou organisations internationales)
  - Les États membres ont **2 ans pour se mettre en conformité.**

5. La cybersécurité en Europe

En Europe : la directive NIS et le RGPD

- Sont un ensemble de mesures techniques et organisationnelles afin de :
  - « gérer les risques qui menacent la sécurité des réseaux et des systèmes » *(art. 14 de la directive NIS)*,
  - « garantir les droits et libertés de la personne concernée » *(art. 5 du RGPD)*
  - « garantir un niveau de sécurité adapté au risque (…) et assurer la sécurité du traitement » *(art. 32 du RGPD)*
- Impliquent amendes/peines de prison si non respectés

5. La cybersécurité en Europe

Données personnelles : RGPD

- Règlement général (européen) sur la protection des données adopté depuis avril 2016

- Applicable et donc **sanctionable à partir de mai 2018** (abroge donc la loi sur la protection des données (européenne) de 1995 et en France celle « informatique et libertés » de 1978+l'adaptation à celle européenne en 2004

« *La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un* ***droit fondamental****. L'article 8, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne (…) et l'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne disposent que* ***toute personne a droit à la protection des données à caractère personnel la concernant.***»

5. La cybersécurité en Europe

RGPD : application

- Les principes relatifs aux **traitements de données à caractère personnel** sont conservés :

  → licéité, proportionnalité, loyauté et transparence des traitements, finalité déterminée, adéquation des traitements, conservation pour une durée limitée et sécurité des données, etc.

- De **nouvelles notions** sont ajoutées :

droit à l'oubli, droit à la portabilité, « privacy by design », profilage, analyses d'impact

- Applicable aux traitements automatisés ou manuels, situés en UE, et/ou sur des citoyens de l'UE (peu importe le siège de l'entreprise). Sont concernés **également les sous-traitants**.

  → Mais pas applicable aux :

  - activités personnelles « domestiques »
  - activités des autorités compétences vis-à-vis des infractions pénales

5. La cybersécurité en Europe

RGPD et droits des personnes :

- Le consentement de la personne concernée/ des enfants
- Le droit à l'information
- Les droits d'accès aux données, de rectification et à l'oubli numérique (ou droit à l'effacement des données)
- Le droit à la limitation du traitement
- **Le droit à la portabilité des données**

5. La cybersécurité en Europe

RGPD *:* Le droit à la portabilité des données (art. 20)

Afin de pouvoir changer de prestataire dans de bonnes conditions :

- Obligation de fournir les données dans un **format ouvert et structuré**,
- Possibilité de transmettre les données **directement d'un prestataire à l'autre**,

5. La cybersécurité en Europe

RGPD : Les obligations du responsable de traitement

- La notion de responsabilité (« accountability ») (art 5 et 24)
- La protection des données dès la conception ou “privacy by design” (art. 25)
- Les règles de profilage (art. 22)
- **L’obligation de sécurité (art. 32 à 34)**
- Les analyses d’impact relatives à la protection des données (art. 35)

5. La cybersécurité en Europe

L'obligation de sécurité (RGPD et NIS)

Assurer la sécurité technique et physique des données :

- **Mesures techniques** et organisationnelles adaptées pour faire face aux activités illicites mais aussi aux dégâts accidentels
  - Guides **ANSSI** (hygiène, bonnes pratiques type chiffrement, disponibilité, confidentialité, résilience,...)
  - Guides **CNIL** (sécurité des données personnelles, pseudonymisation,…) + procédure de vérification de leur efficacité
  - En cas de contrôles c'est la conformité à ces référentiels qui est contrôlée

- En cas de faille **notifier aux** autorités de contrôle (ANSSI, CNIL, ARS,... **72h après prise de connaissance au plus tard**) en mettant en place une **procédure de notification et d'analyse** constante de l'efficacité des mesures mises en œuvre (art. 33 RGPD et 14,16,20 NIS):

→ communiquer nature/volumétrie, conséquences, mesures prises et contact local

- Et prévoir de **rétablir l'accès et la disponibilité** des données dans des délais « appropriés »

Tout ceci nuancé par les :
- connaissances actuelles,
- moyens disponibles
- catégories de données traitées

5. La cybersécurité en Europe

Opérateurs de services essentiels et fournisseurs de services NIS :

- Les « OSE », précisés par l'UE (environ 600 en France avec les OIV)
  - Tributaires de systèmes d'information essentiels (SIE), *contrairement au OIV qui n'en ont pas forcément*
- Les fournisseurs de services NIS
- … et leurs partenaires (sous-traitant, coresponsable de traitement,..)

→ Appliquent les mesures de l'arrêté du 14/9/2018 (principes de sécurité) et testent, analysent, évaluent régulièrement leur efficacité au moyen d'audits réguliers (art. 32 RGPD et 15,16 NIS). Cela implique des clauses spécifiques dans les contrats.

6. Le droit des T.I.C. et l'organisation de la cybersécurité en France

e. Le rôle de la CNIL : La protection des données à caractère personnel

CNIL. Autorité de contrôle (Art. 51 à 59 du RGPD)

Autorité de contrôle indépendante, en charge de l'application du règlement en France (et de manière générale dans le pays du siège de l'entreprise).

Elle **sensibilise** le public et **conseille** le gouvernement/parlement.

Traite les **réclamations** (personnes ou organismes)

Coopère avec ses **homologues européens**.

6. Le droit des T.I.C. et l'organisation de la cybersécurité en France

e. Le rôle de la CNIL : La protection des données à caractère personnel

Pouvoir élargis avec le RGPD (Art 58):

Enquête et audit avec **tous pouvoirs** sur la mise à disposition des documents et données mis à disposition

Notifie les violations, **ordonne la mise en conformité** (en imposant une **limitation ou interdiction de traitement**)

Impose une **amende administrative** (jusqu'à 10 à 20 millions d'€ et de 2 à 4 % du CA **mondial** de l'exercice précédent)

Ex : arrêt de l'envoi de données à un pays tiers

6. Le droit des T.I.C. et l'organisation de la cybersécurité en France

DPO/DPD : Délégué à la protection des données (art. 37 à 39)

- remplace le correspondant informatique et libertés – CIL (loi Informatique et Libertés)
- **uniquement pour** les entreprises ayant pour "activité de base" la gestion de données personnelles "à grande échelle" ou le contrôle et suivi du comportement des personnes (y compris le profilage).

7. La cybersécurité à l'international

RGPD : Transfert de données entre pays

- Possibles entre **pays membres de l'UE**
- et pays **non membres** (Argentine, Canada, Guernesey, Ile de Man, Israël, Nouvelle-Zélande, Suisse, Urugay,…) **satisfaisant aux critères du RGPD (art. 45)**
- Pour les **Etats-Unis, seules les sociétés ayant choisi de se conformer aux principes du Privacy Shield** (adéquation négociée, invalidé par l'UE le 16/7/2020, arrêt SCHREMS2) étaient concernées (a remplacé Safe Arbor) et soumises à contrôles annuels:
  - accès aux données personnelles par les autorités américaines encadré et transparent.
  - accès généralisé aux données est expressément interdit (**Code du commerce vs Patriot Act et Cloud Act ?**)

Exceptions à l'interdiction : consentement explicite (ou incapacité de la personne), intérêts vitaux, justice, intérêt public, contrat (achat).

7. La cybersécurité à l'international

États-Unis

- Un référentiel sur la cybersécurité fourni par l'**institut national des normes et technologies** (NIST, 2013),
- Un référentiel pour l'évaluation de la maturité des organisations en cyber-résilience du **département de la sécurité intérieure** (DHS, 2016),
- Une **directive CISA** qui crée un cadre juridique encourageant l'échange entre secteur privé et gouvernement, associée à la création d'une **nouvelle agence dédiée cybersécurité CTIIC** (2015)
- La stratégie du **département de la défense** (DoD) qui inclut l'apport de l'IA/cyber (2019à

7. La cybersécurité à l'international

Royaume-Uni

- Stratégie donnée par le centre national cyber (NCSC, 2016)
- Jugent le RGPD un bon levier

Japon

- Plan stratégique en cybersécurité donné par le centre national de préparation contre les incidents et de la stratégie de sécurité (NISC, 2015)

Chine

- Loi fondamentale sur la cybersécurité par le congrès du peuple chinois pour sa souveraineté et le développement « sain » des TIC (2017)

CyberEdu

La sécurité par l'enseignement supérieur des NTIC

Merci de votre attention