# Organisation de la Sécurité Informatique en France

Yannick Chevalier
Université de Toulouse
CSA M1, Security

# Plan

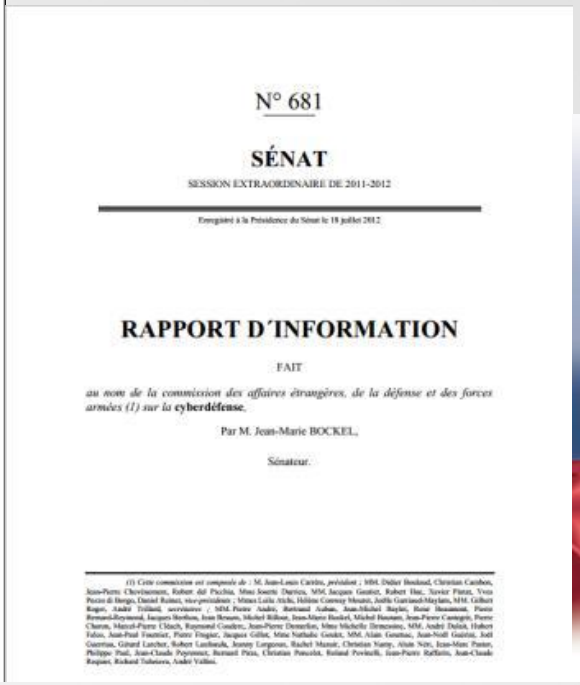

## Organisation de la cybersécurité en France

## Législation

## Cybercriminalité

## Protection des données personnelles

# CYBERDÉFENSE



N° 681

SÉNAT

SESSION EXTRAORDINAIRE DE 2011-2012

RAPPORT D'INFORMATION

FAIT

*au nom de la commission des affaires étrangères, de la défense et des forces armées (1) sur la* **cyberdéfense**,

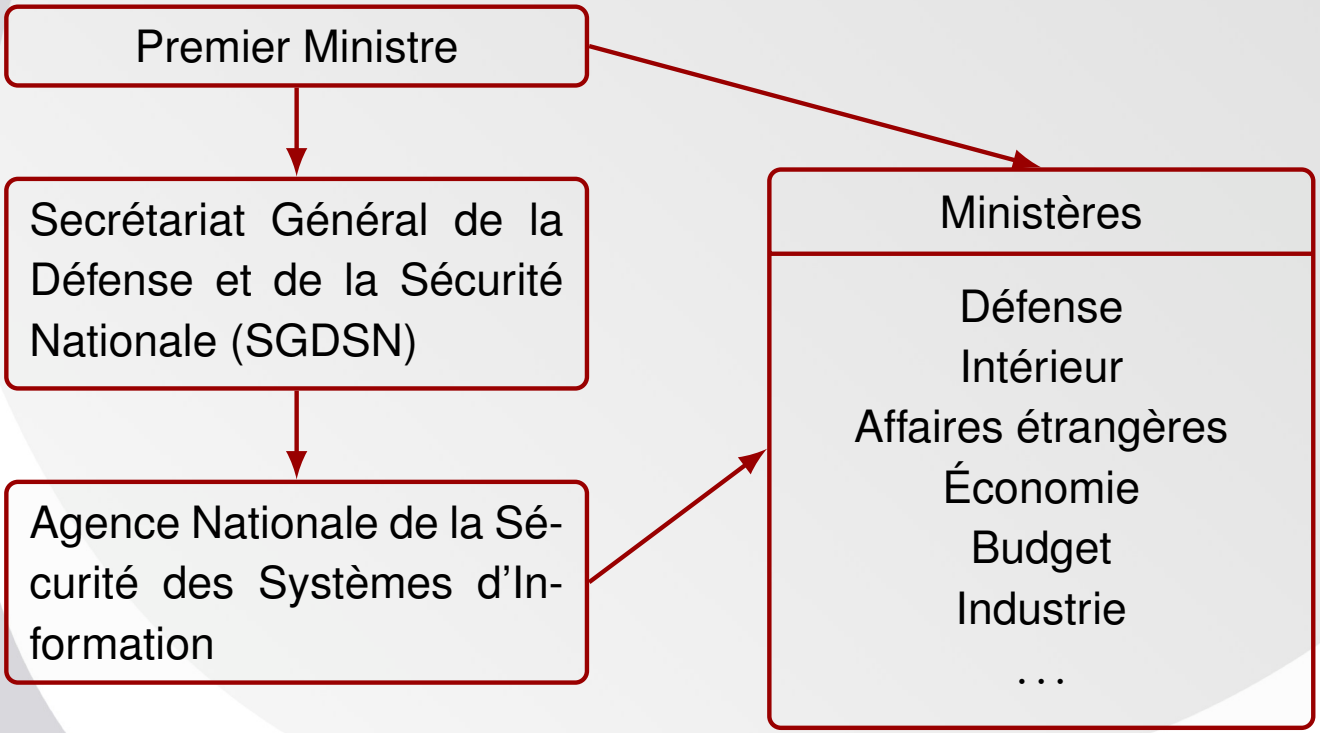
Par M. Jean-Marie BOCKEL,

Sénateur.


## PRINCIPAUX POINTS

- cyberattaques, une menace majeure
- besoin d'un effort marqué (libre blanc 2013)

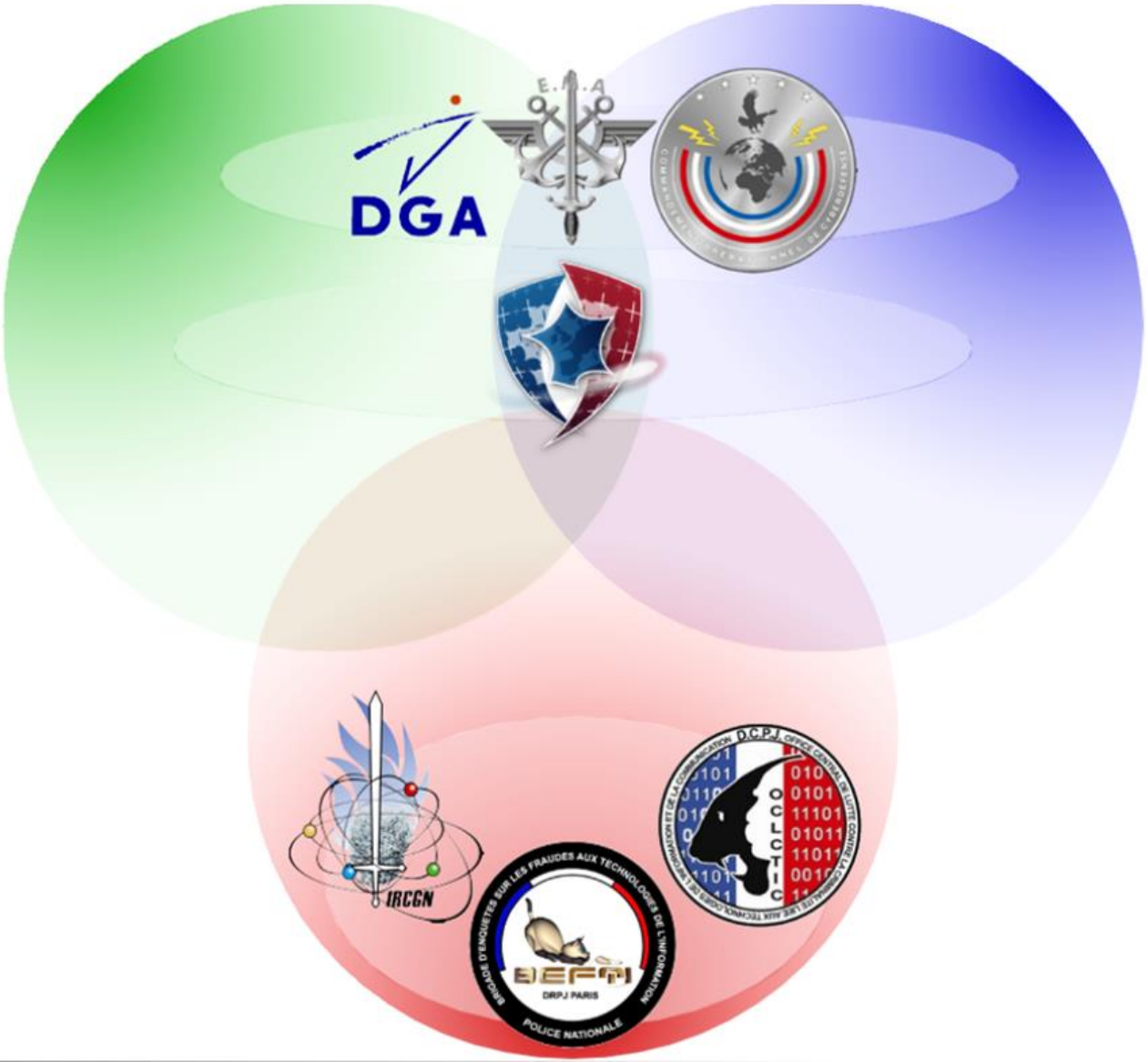
# Organisation de la sécurité en France




**Hauts fonctionnaires de défense et de sécurité (HFDS) :** préparation, coordination des mesures de défense, chargés de la sécurité des SI

# CYBERSÉCURITÉ

**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"

# Plan

Organisation de la cybersécurité en France

Législation

Cybercriminalité

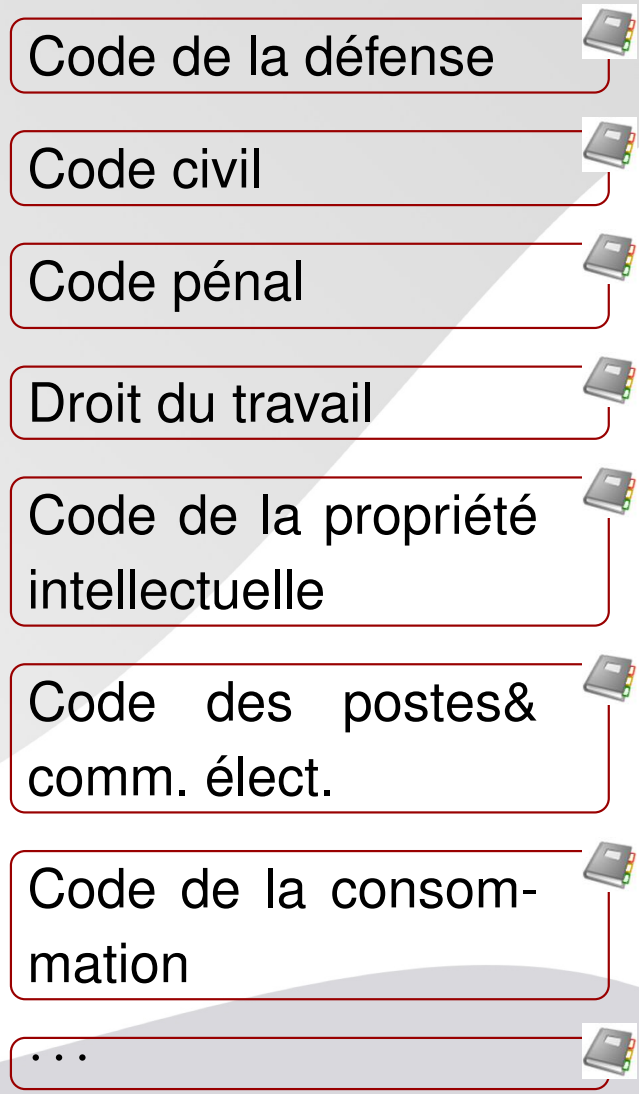
Protection des données personnelles

# Domaines couverts

- Liberté d'expression
- Protection du *e*-commerce
- Propriété intellectuelle
- Protection de la vie privée
- protection des entreprises
- Cybercriminalité
- ...

# TEXTES LÉGAUX

- 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
  - beaucoup de jurisprudence
- besoin d'un effort de veille juridique



# Plan

Organisation de la cybersécurité en France

Législation

Cybercriminalité

Protection des données personnelles

# LUTTE CONTRE LA CYBERCRIMINALITÉ

## DÉFINITION

Ensemble des actes contrevenants aux traités internationaux ou aux lois nationales utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible.

## INVESTIGATION NUMÉRIQUE (FORENSICS)

Ensemble des protocoles et de mesures permettant de rechercher des éléments techniques sur un conteneur de données numériques en vue de répondre à un objectif technique en respectant une procédure de préservation du conteneur.

# État de la législation (1/2)

## Loi Godfrain du 05/01/1988

L'accès ou le maintien frauduleux dans tout ou partie d'un système de traitement automatisé des données (STAD), art. 323-1 du code pénal, est puni de 2 ans d'emprisonnement et de 30.000€ d'amende au maximum.

## Commentaires

- élément matériel de l'infraction : accès ou maintien
- fraude ou l'élément moral : être connaissance d'être sans droit et en connaissance de cause

## Jurisprudence

- définition des STAD : réseau d'un fournisseur, réseau bancaire, disque dur, radio, téléphone, site internet,...
- tendance des tribunaux : plus grande intransigeance envers les hébergeurs ne protégeant pas assez les données de leurs utilisateurs

# État de la législation (2/2)

## Article 323-2 du code pénal

Entraver ou fausser le fonctionnement d'un STAD est puni d'un maximum de 5 ans d'emprisonnement et de 75.000€ d'amende

## Article 323-3 du code pénal

L'introduction, la suppression ou la modification frauduleuse de données dans un STAD est puni d'un maximum de 5 ans d'emprisonnement et de 75.000€ d'amende

## Article 323-3-1 du code pénal

Importer, détenir, offrir, céder, mettre à disposition sans motif légitime un programme ou un moyen permettant de commettre une de ces infractions est puni de la même peine

- Art. 323-4 : association de malfaiteurs en informatique
- Art. 323-5 : peines complémentaires
- Art. 323-6 : responsabilité pénale des personnes morales
- Art. 323-7 : répression de la tentative

# Plan

Organisation de la cybersécurité en France

Législation

Cybercriminalité

Protection des données personnelles

# Rôle de la CNIL

## Origine

Loi du 06/01/1978 relative à l'informatique, aux fichiers, et aux libertés

## Champ d'application (Art. 2)

La présente loi s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers, à l'exception des traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles, lorsque leur responsable remplit les conditions prévues à l'article 5 (relevant du droit national).

## Qu'est-ce qu'une donnée à caractère personnel ?

Constitue une donnée à caractère personnel 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 sont propres.

# Protection des données à caractère personnel

## Traitement loyal et licite

- les données sont collectées pour des finalités déterminées explicites et légitimes
- de manière proportionnée (adéquates, pertinentes, et non excessives)
- avec le consentement de la personne concernée (sauf exception)
- pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités

## Droits des personnes physiques sur leurs données

- Un droit d'information préalable au consentement
- Un droit d'accès aux données collectées
- Un droit de rectification
- Un droit dopposition pour raison légitime

# Obligations administratives

## Déclaration préalable (Art. 22 à 24)

- Le traitement peut faire l'objet d'une dispense de déclaration
- Le traitement échappe à l'obligation de déclaration car le responsable du traitement a désigné un correspondant à la protection des données (CIL)
- Dans tous les autres cas, le traitement doit effectivement faire l'objet d'une déclaration préalable

## Autorisation préalable (Art. 25 à 27)

- pour les traitements sensibles listés à l'article 25
- examen par la CNIL sous deux mois (whitelisting, rejet si pas de réponse positive)

# Obligations de confidentialité et de sécurité

## Pour l'opérateur principal

- mise en œuvre des mesures techniques et organisationnelles appropriées, au regard de la nature des données et des risques, pour préserver leur sécurité
- sécurité : empêcher qu'elles soient déformées, endommagées, ou que des tiers non-autorisés y aient accès
- pas de techniques précisés dans le texte, mais un guide de sécurité est publié par la CNIL

## Pour les sous-traitants

- ils doivent apporter les mêmes garanties que l'opérateur principal
- sous la responsabilité de l'opérateur principal

# Peines prévues

## Sanctions pénales

- Douze délits punis de 3 à 5 ans d'emprisonnement et jusqu'à 300.000€ d'amende
- obligations de sécurité « Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000€ d'amende »

## Sanctions civiles

Dommages-intérêts en fonction du préjudice causé aux personnes concernées

## Sanctions administratives par la CNIL

- injonction de cesser le traitement pour les fichiers soumis à déclaration ou de retrait de l'autorisation accordée
- sanction pécuniaire
- interruption de la mise en œuvre du traitement ou verrouillage des données pour 3 mois
- publicité des avertissements et, en cas de mauvaise foi, pour les autres sanctions