ENJOY SAFER TECHNOLOGY™

Livre blanc écrit
en collaboration avec

**Maître ITEANU,**

avocat à la Cour et
spécialisé en droit de
l'informatique.

# LIVRE BLANC :

## La Cybersécurité dans le contexte européen.

## Nos conseils avant 2018 !

# SOMMAIRE

# Éditorial : prendre sa cybersécurité en main, une obligation légale

ITEANU
Société d'Avocats | Law Office

Pour qui suit l'actualité de la cybersécurité en Europe, 2016 aura été une année bien remplie.

Impossible bien sûr de passer sous silence le règlement européen sur les données personnelles publié au Journal Officiel de l'Union européenne le 4 mai 2016, plus connu sous l'acronyme « RGPD » en français, ou « GDPR » en anglais.

Au menu, des sanctions alourdies à la disposition des CNIL européennes, jusqu'à 4% du chiffre d'affaires mondial, l'instauration d'un Délégué à la Protection des Données dit DPO obligatoire dans le secteur public et pour les traitements les plus sensibles, la responsabilité des sous-traitants désormais possible au même titre que le responsable des traitements, la notification obligatoire des violations des données personnelles à la CNIL sous 72 heures pour tous…

Le RGPD sera applicable automatiquement dans les États européens le 25 mai 2018, ce qui laisse peu de temps d'adaptation.

Toujours au niveau européen, la Directive NIS pour *Network and Information Security*, adoptée le 6 juillet 2016, est le second texte d'importance de cette année charnière.

Cette Directive apporte également d'importants changements avec la consécration d'une législation à part entière sur la protection des systèmes d'information. On peut la lire comme une sorte de code de la cybercriminalité, que les législateurs des États membres vont devoir transposer avant le 9 mai 2018.

Enfin, le législateur n'est pas en reste, avec l'adoption de la loi pour une république numérique, en vigueur depuis le 7 octobre 2016. Ici, c'est le droit à l'oubli pour les mineurs qui est instauré, les sanctions de la CNIL qui passent de 150.000 euros à 3 millions d'euros en attendant le RGPD vu ci-avant, la création d'un nouveau délit le *porn revenge*, la portabilité des données au bénéfice des consommateurs à la charge des plateformes qui est imposée, et un statut de hacker blanc pour qui découvre une faille de sécurité et la signale à l'ANSSI sans grand risque de poursuites pénales à son encontre.

Comme on le voit, l'ambiance est dans l'activisme pour le droit des technologies de l'information, qui s'insère dans toutes les sphères de la vie professionnelle et personnelle des personnes physiques et des organisations. On est clairement passé d'une attitude passive face au risque cybercriminel, sur la confidentialité et la sécurité des données personnelles, à une attitude proactive, c'est la cybersécurité.

C'est dans ce contexte que cet ouvrage est d'importance. Plutôt que de lister un guide détaillé des nouveaux principes énoncés, il cherche à dessiner les grandes tendances qu'il faut retenir et qui aideront l'entreprise à se rendre conforme au présent et à l'avenir.

Cet ouvrage est aussi le fruit d'une collaboration entre la technique, l'organisation et le droit. Un couple à trois aujourd'hui, incontournable.

**Olivier ITEANU**
**Avocat à la Cour**

# 2016, l'année de la règlementation européenne en matière de sécurité informatique

## Vue d'ensemble par une approche terminologique

**La cybersécurité n'est pas née en 2016.**

Les questions de cybercriminalité sont apparues en France, dans le droit, avec la loi Godfrain de janvier 1988, du nom du Député Jacques Godfrain, qui l'avait proposé.

Elle instaure les premiers délits informatiques. Il était à l'époque question de « fraude informatique », dans la mesure où l'informatique communicante et l'Internet n'étaient pas encore arrivés dans le grand public.

On retrouve aujourd'hui la loi Godfrain codifiée aux articles L 323-1 et suivants du Code pénal. Ces dispositions restent, même avec les nouveaux textes de 2016, la pierre angulaire des délits informatiques. Il s'agit essentiellement de l'accès ou du maintien frauduleux dans le système informatique, d'entraver ou de fausser son fonctionnement et d'introduire, modifier, supprimer et, depuis fin 2014, extraire illicitement toutes données du SI.

La fraude informatique a ensuite laissé sa place à la cybercriminalité, marquant ainsi l'arrivée en force d'Internet sur et autour duquel nos sociétés s'organisent. Des délits spécifiques aux réseaux numériques ont été créés comme le délit aggravé de pédopornographie réalisé en réseaux ou l'usurpation d'identité numérique.

Le premier Traité international de Cybercriminalité date de novembre 2001. Il s'agit de la Convention de Budapest sur la cybercriminalité.

Mais le terme cybercriminalité laisse à penser que la réponse au phénomène est exclusivement judiciaire et pénale, en raison de l'emploi du mot « criminel ».

**La cybersécurité parachève cette évolution.**

Le changement « cybersécurité » illustre parfaitement que le phénomène doit être combattu avant l'acte criminel, par l'instauration au sein des organisations de mesures d'ordre techniques, organisationnelles donc humaines et juridiques.

Sur ce dernier point, le contrat, l'organisation interne (chartes informatiques et/ou Internet) et les audits juridiques participent à la lutte contre ce phénomène.

L'année 2016 aura accentué ce mouvement, comme nous allons le présenter ci-après.

Dans ce contexte, le paysage législatif voit apparaître en 2016 de nouvelles mesures éparses qui viennent s'ajouter aux textes anciens sans les faire disparaître.

Voici donc les trois textes de loi de l'année 2016 qui vont durablement influencer la cybersécurité pour les cinq années à venir :

**27 avril 2016**

Adoption du « règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la Directive 95/46/CE » dit règlement RGPD.

**Application : 25 mai 2018**

**06 juillet 2016**

Adoption de la « Directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information » dite Directive « NIS ».

**Application : 9 mai 2018**

**07 octobre 2016**

Loi pour une république numérique adoptée le 7 octobre 2016.

**Application : immédiate**

Enfin, pour être complet, le numérique s'invite désormais dans chaque projet de loi ou presque.

Ainsi, à titre d'exemple :

- La loi relative à la liberté de création du 7 juillet 2016 prévoit de faire payer une redevance à tous « services automatisés de référencement d'images » qui reproduiraient les images dans leur liste de résultats (autrement dit les moteurs de recherche)[1].
- La loi prorogeant l'état d'urgence du 21 juillet 2016 précise notamment les règles de la saisie de données informatiques dans le cadre de perquisitions.
- La loi dite Sapin II du 9 décembre 2016 crée le statut protecteur et protégé de lanceur d'alerte défini comme « … une personne physique qui révèle de manière désintéressée et de bonne foi, un crime ou un délit (…) ou une menace ou un préjudice graves pour l'intérêt général … ». Ces dispositions peuvent parfaitement concerner un délit numérique, par exemple en matière de données personnelles.

**En conclusion,** la protection des systèmes d'information connaît désormais un foisonnement de textes divers et épars.

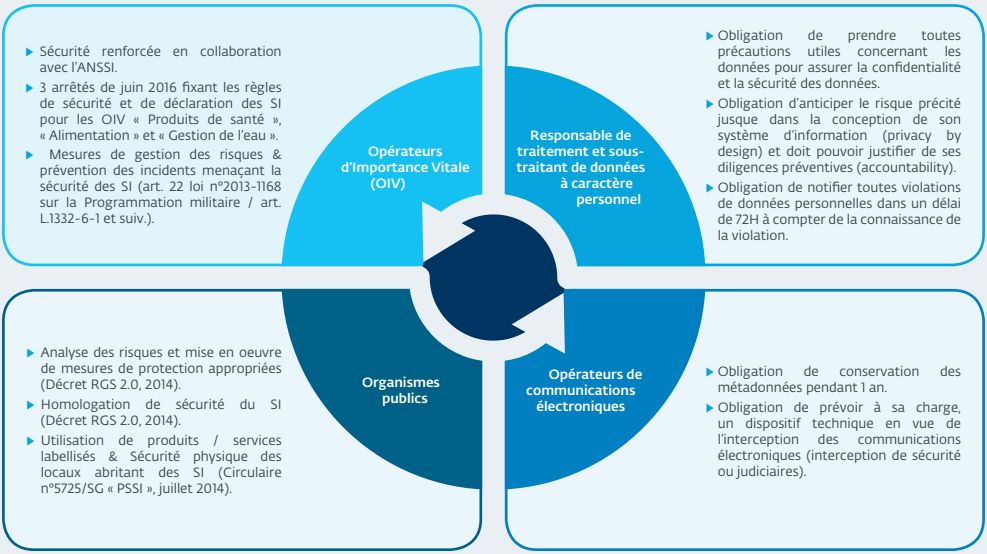
Bien évidemment, certains textes légaux généraux concernent tous types d'organisations. C'est le cas pour :

- Les délits informatiques de base issus de la loi Godfrain, notamment les délits d'accès et de maintien frauduleux, l'entrave aux systèmes et les extractions illicites de données (art. 323-1 et suivants du Code pénal).
- Le délit d'usurpation d'identité numérique (art. 226-4-1 du Code pénal).

**1.** Art. 30 de la loi n° 2016-925 du 7 juillet 2016 relative à la liberté de la création, à l'architecture et au patrimoine, modifiant les art. L136-1 et suiv du code de la propriété intellectuelle

Mais dans certains cas, ces textes s'adressent à une population particulière d'organisations (par exemple les Opérateurs d'Importance Vitale - OIV - ou les opérateurs ex télécoms) ou à toutes organisations qui développent certaines activités (par exemple en matière de données personnelles).

Nous résumons selon le schéma ci-après, les grandes obligations incombant à quatre types d'acteurs directement concernés par la cybersécurité, ces catégories pouvant se cumuler.




Ce livre blanc présente principalement les deux textes phares de l'année 2016 en matière de cybercriminalité : le RGPD et la Directive NIS.

Contrairement au RGPD qui est d'application immédiate sans modification ni adaptation de son texte dans les législations nationales des pays de l'UE, la Directive NIS fixe des objectifs aux États membres et nécessite une « transposition » dans les législations nationales. Il est en conséquence plus complexe d'évaluer l'impact réel de la Directive NIS.

Par ailleurs, ces deux textes ont été écrits concomitamment et en concertation. Cette volonté ne peut qu'être saluée puisque visant à limiter toute possibilité de contradiction.

Ils apparaissent majeurs quant à leur influence sur l'appréhension par les entreprises des risques d'atteinte à leur système d'information. Ils mettent désormais l'accent sur la prévention des cyber-risques pour les entreprises. Leurs champs d'applications sont vastes et touchent un grand nombre d'acteurs économiques directement ou indirectement.

Au-delà de leur champ d'action, ces deux textes imposent des obligations inédites que nous détaillons ci-après.

## Le RGPD, un renforcement en matière d'obligation de sécurité des données à caractère personnel

Le règlement européen du 27 avril 2016 dit « RGPD » est l'évènement de l'année 2016. Il vient apporter des modifications majeures à la Directive 95/46/CE d'octobre 1995 relative à la protection des données à caractère personnel qu'il remplace, et comporte des mesures spécifiques à la sécurité des données à caractère personnel.

**À noter :**

- 173 considérants & 99 articles.
- Concerne uniquement le traitement des données personnelles.
- Abroge la Directive 95/46/CE à partir du 25 mai 2018.
- Mais conserve les principes de base de la loi « Informatique et Libertés » de 1978 en les renforçant, en les sanctionnant davantage et en créant de nouveaux droits pour les citoyens.
- Met fin au système de déclaration auprès de la CNIL.
- Instauration d'un Délégué à la Protection des Données (DPO).

Le RGPD consacre trois articles spécifiques à la sécurité des données à caractère personnel :

- Article 32 « Sécurité du traitement ».
- Article 33 « Notification à l'autorité de contrôle d'une violation de données ».
- Article 34 « Communication à la personne concernée d'une violation de données ».

### Qui est concerné ?

Le RGPD vise spécifiquement le responsable d'un traitement de données à caractère personnel ou son sous-traitant[2], dans le cadre des activités d'un établissement sur le territoire de l'Union, « que le traitement ait lieu ou non dans l'Union. »[3].

Deux nouveautés majeures sont à noter :

- **Le sous-traitant est désormais directement responsable** en raison des nouvelles obligations imposées par le RGPD, notamment :
  - l'obligation de sécurisation des données au même titre que le responsable de traitement[4]
  - l'obligation de notification au responsable de traitement en cas de violation des données à caractère personnel[5]
  - l'obligation d'informer et de demander l'autorisation au responsable de traitement si le sous-traitant fait lui-même appel à des sous-traitants
  - l'obligation de se conformer aux garanties prescrites par le règlement en matière de transfert de données à l'étranger, au même titre que le responsable de traitement

**2.** Nouveauté 2018
**3.** Art. 2 et 3 RGPD
**4.** Art. 32-1 RGPD
**5.** Art. 33 RGPD

Le responsable de traitement reste cependant responsable des actes de son sous-traitant, leur relation étant régie par contrat.

- **Le champ d'application s'élargit aux sociétés étrangères.** Ainsi, les règles de protection des données à caractère personnel s'appliquent[6] :
  - que le traitement ait lieu ou non dans l'UE, tant qu'il s'inscrit dans le cadre de l'activité d'un établissement d'un responsable de traitement et/ou d'un sous-traitant sur le territoire de l'UE
  - même si l'entreprise n'est pas établie dans l'UE, sont également concernées toutes entreprises qui effectuent le traitement de données à caractère personnel. Pour cela, les activités doivent être liées à l'offre des biens ou services, ou au suivi des comportements des personnes se trouvant sur le territoire de l'UE

### Notion d' « établissement » :

En 2015, la CJUE a défini la notion « d'établissement » au sens de la Directive 95 comme « toute activité réelle et effective, même minime, exercée au moyen d'une installation stable ».

Cette définition implique un grand nombre d'entreprises étrangères, que leur siège soit en Europe ou non, tant que leur activité de traitement des données est liée aux activités de leur établissement en Europe.

Par exemple seront concernés les sites Internet dédiés aux utilisateurs européens.

## Quelles mesures adopter ?

La garantie de sécurité des données personnelles est désormais un principe ancré dans le règlement européen à l'article 5 :

> « *Les données à caractère personnel doivent être [...] traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité)* ».

Le RGPD impose aux responsables de traitement et à leurs sous-traitants d'analyser les risques potentiels d'atteinte à leur traitement, de prendre les mesures préventives en conséquence, et enfin, en cas d'atteinte, de prendre les dispositions adéquates :

- Avant le traitement par la réalisation d'une analyse d'impact afin de cibler les risques potentiels.
- Par la désignation d'un délégué à la protection des données dans certains cas.
- Obligation de sécuriser le traitement des données personnelles.
- Obligation de notification de violation des données à caractère personnel dans les 72h à l'autorité de contrôle et à la personne concernée (article 33 et 34).

### 1. Réalisation d'une analyse d'impact[7]

Lorsqu'un traitement « est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques », le responsable de traitement doit effectuer, avant le traitement, une analyse de l'impact des opérations de traitement envisagées.

Cette analyse d'impact est obligatoire dans les cas suivants :

> *« a) L'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire.*
>
> *b) Le traitement à grande échelle de catégories particulières de données visées à l'article 9 paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 .*
>
> *c) La surveillance systématique à grande échelle d'une zone accessible au public ».*

Enfin, la CNIL établit et publie une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise.

### 2. La désignation d'un délégué à la protection des données

Les responsables de traitement et leurs sous-traitants devront désigner un délégué à la protection des données (DPO) :

- S'ils appartiennent au secteur public.
- Si leur activité principale nécessite un suivi régulier du fait de leur nature, leurs portées et/ou leur finalité.
- Si les données traitées sont considérées comme « sensibles » (comme les données de santé, de religion…) ou portent sur certaines condamnations pénales ou infractions.

Sa désignation devra être fondée sur ses qualités professionnelles et notamment ses connaissances du droit et des *« pratiques en matière de protection de données »* [8]. Le DPO doit *« dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci »*[9].

### 3. Obligation de sécuriser le traitement des données personnelles

Suite à l'analyse d'impact des risques, le responsable de traitement et son sous-traitant sont désormais dans l'obligation de mettre en place plusieurs mesures et ce dès la conception du traitement, c'est la notion de « privacy by design » :

- Des moyens permettant de *« garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ».*
- Des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique.
- Une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

**6.** Art. 03 RGPD
**7.** Art. 35 RGPD
**8.** Art. 37 RGPD
**9.** Art. 39 RGPD

Parmi les mesures de protection que peuvent prendre les responsables de traitement et leurs sous-traitants en amont, le règlement encourage sur certaines mesures jugées « suffisantes » pour sécuriser le traitement de données à caractère personnel :

- L'application d'un **code de conduite** approuvé : le RGPD encourage la rédaction de codes de conduite par secteur d'activité. Cependant à ce jour, les auteurs et conditions de leur rédaction ne sont pas encore déterminés.
- **La pseudonymisation** est une mesure préventive permettant d'assurer la sécurité des données à caractère personnel[10].

> **Définie comme** *« le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable »*

- **Le chiffrement** est reconnu comme un moyen de garantir la sécurité des données[11].

> **Défini comme** des *« mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès »*

### 4. Les obligations en cas d'atteinte aux données à caractère personnel

La violation des données est définie par le RGPD comme *« une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données »*[12].

Lorsque la violation est caractérisée, il est nécessaire :

- **D'avertir la CNIL dans les 72h de la violation des données à caractère personnel.** Désormais, l'obligation de notification de failles de sécurité n'incombe plus qu'au responsable de traitement, mais également au sous-traitant vis-à-vis du responsable de traitement, et devra être notifiée à la CNIL dans un délai maximum de 72h *« au plus tard après avoir pris connaissance* [de la violation] »[13].

  La notification devra contenir les informations suivantes :

  - la description de la nature de la violation (y compris si possible le nombre approximatif de personnes et de données susceptibles d'être concernées)
  - le nom et les coordonnées du délégué à la protection des données
  - les conséquences probables de la violation et les mesures prises ou qui seront prises pour remédier à cette violation ou atténuer ses conséquences
  - les mesures prises ou que le responsable de traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives

Une exemption existe néanmoins si la violation de sécurité en question n'est pas susceptible d'engendrer un risque pour les « droits et libertés des personnes physiques ». Il revient donc aux entreprises d'apprécier les conséquences de l'atteinte du traitement de données avant de la notifier.

- **Pour le sous-traitant qui a connaissance de cette violation, d'avertir le responsable de traitement dans les meilleurs délais.**
- **D'avertir les personnes concernées par la violation des données** lorsque cette violation est susceptible d'engendrer des risques élevés pour ces dernières. La notification devra contenir les mêmes informations que pour la notification CNIL.

  Le responsable de traitement peut cependant être exempté de cette notification à la personne s'il remplit l'une des conditions suivantes :

  - **le responsable de traitement a mis en œuvre les mesures de protection technique et organisationnelle appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement**
  - le responsable de traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées n'est plus susceptible de se matérialiser
  - si cette communication exigeait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace

## La Directive « NIS » visant à la sécurité des systèmes d'information

La Directive du 6 juillet 2016 dite « NIS » traite pour la première fois exclusivement de la protection des systèmes d'information.

La Directive NIS a pris le soin de définir la « *sécurité des réseaux et des systèmes d'information* » comme « *la capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles* ».

### Qui est concerné ?

**À noter :**

La Directive NIS ne s'applique pas « *aux microentreprises et petites entreprises* », c'est-à-dire qu'elle ne concerne que **les sociétés de plus de 250 personnes et de plus de 50 millions d'euros de chiffre d'affaires.**

**10.** Considérant 28 du RGPD
**11.** Art. 6 et 32 du RGPD
**12.** Art. 4.12 du RGPD
**13.** Art. 33 du RGPD

La Directive NIS touche deux catégories d'entités, considérées comme des acteurs majeurs pour le bon fonctionnement et la sécurité des réseaux et des systèmes d'information :

- Les **Opérateurs de services essentiels (OSE)** qui sont définis comme des entités publiques ou privées travaillant dans les secteurs suivants : transport, banque, infrastructure de marchés financiers, secteur de la santé, fourniture et distribution d'eau potable et infrastructure numérique[14].
- Les **Fournisseurs de services**, définis comme des « personne(s) morale(s) qui fourni(ssent) un service numérique »[15] et plus spécifiquement, il est renvoyé à une annexe qui précise les services numériques visés.

  Ces derniers sont :

  - **les places de marché en ligne :** c'est-à-dire les services de traitement de transactions, d'agrégation de données ou de profilage d'utilisateurs[16]
  - **les moteurs de recherche en ligne :** définis par la Directive comme un service numérique permettant aux utilisateurs de faire des recherches[17]
  - **les services d'informatique en nuage :** définis par la Directive comme des services *« qui permettent l'accès à un ensemble modulable et variable de ressources informatiques pouvant être partagées »* et couvre selon elle un *« vaste éventail d'activités »* tel que *« les réseaux, serveurs, et autres infrastructures, le stockage, les applications et les services »*[18]

Il apparaît ainsi que le terme *« fournisseur de services »* visé par la Directive NIS regroupe un panel extrêmement large d'entreprises, allant de la plateforme de transactions jusqu'aux hébergeurs de données.

**Attention !**

Les Fournisseurs de services numériques qui ne sont pas établis dans l'UE, mais qui fournissent les services énumérés ci-après à l'intérieur de l'UE, doivent désigner un représentant dans l'Union.

Le Fournisseur est considéré comme relevant de la compétence de l'État membre dans lequel le représentant est établi (Art. 18 de la Directive NIS).

## Quelles mesures adopter ?

Les obligations préconisées par la Directive NIS couvrent toutes les étapes de la sécurisation des systèmes d'information, de la prévention à la gestion d'une éventuelle attaque, c'est-à-dire :

- Avant l'atteinte au système d'information avec de nombreuses mesures préventives.
- Après l'atteinte au système d'information.

### 1. Les obligations de prévention

La Directive NIS précise que les fournisseurs de services entrant dans son champ d'application devront :

- **Réaliser un audit interne d'identification des risques liés à leur système d'information** en prenant en compte les critères suivants :

  « *a) La sécurité des systèmes et des installations*
  *b) La gestion des incidents*
  *c) La gestion de la continuité des activités*
  *d) Le suivi, l'audit et le contrôle*
  *e) Le respect des normes internationales* »[19]

  À cette fin, le fournisseur de services devra produire un document relatant cet audit, à titre conservatoire. Ce document doit rester confidentiel, il conviendra donc de limiter son accès aux salariés.

- **Prendre des mesures techniques et organisationnelles.** Ces mesures devront être « nécessaires et proportionnées » et permettre de :

  - gérer les risques identifiés
  - « *réduire au minimum l'impact de ces incidents sur les services visés* »
  - « *garantir la continuité de ces services* »

  Ces mesures permettront la continuité du service numérique, essentielle selon la Directive « *pour le bon fonctionnement des entreprises* »[20].

### 2. En cas d'atteinte à la sécurité des réseaux et systèmes d'information

Il est intéressant de noter que la Directive NIS définit les notions d' « Incident » et de « Gestion d'Incident ».

**Incident**

*« tout évènement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d'information ».*

**Gestion d'incident**

*« toutes procédures utiles à la détection, à l'analyse et au confinement d'un incident et toutes les procédures utiles à l'intervention en cas d'incident ».*

Si malgré la mise en place de mesures de protection, un incident sur les systèmes d'information est détecté, les fournisseurs de services entrant dans le champ d'application de la Directive NIS devront :

- **Établir une analyse d'impact.** En cas d'atteinte à leur système d'information, les fournisseurs de services numériques doivent alors mesurer l'ampleur de l'impact, selon les critères suivants :

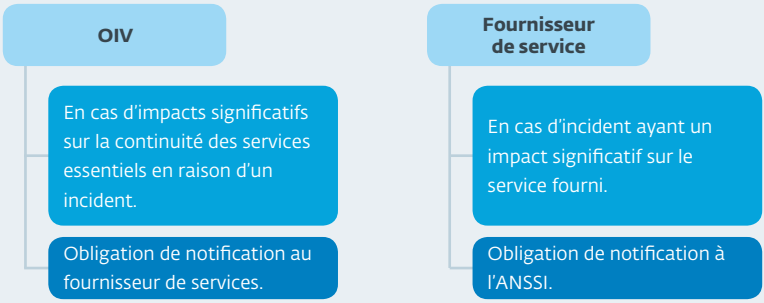
**14.** Art. 4 et Annexe II de la Directive NIS
**15.** Art. 4 Directive NIS
**16.** Considérant 15 Directive NIS
**17.** Art. 4 Directive NIS
**18.** Considérant 15 et Art. 4 Directive NIS
**19.** Article 16 de la Directive NIS « «Les États membres veillent à ce que les fournisseurs de service numérique identifient les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'ils utilisent pour offrir, dans l'Union, les services visés à l'annexe III, et prennent les mesures techniques et organisationnelles nécessaires et proportionnées pour les gérer. Ces mesures garantissent, compte tenu de l'état des connaissances, un niveau de sécurité des réseaux et des systèmes d'information adapté au risque existant et prennent en considération les éléments suivants(....) Les États membres veillent à ce que les fournisseurs de service numérique prennent des mesures pour éviter les incidents portant atteinte à la sécurité de leurs réseaux et systèmes d'information, et réduire au minimum l'impact de ces incidents sur les services visés à l'annexe III qui sont offerts dans l'Union, de manière à garantir la continuité de ces services ».
**20.** Considérant 48 Directive NIS

*« a) Le nombre d'utilisateurs touchés par l'incident, en particulier ceux qui recourent au service pour la fourniture de leurs propres services*
*b) La durée de l'incident*
*c) La portée géographique eu égard à la zone touchée par l'incident*
*d) La gravité de la perturbation du fonctionnement du service*
*e) L'ampleur de l'impact sur les fonctions économiques et sociétales »*

Au vu de ces critères très larges, beaucoup d'évènements peuvent être qualifiés d'« *incidents* ». Un nombre important d'évènements devra donc être notifié à l'ANSSI ou au fournisseur de services.

- **Obligation de notification à l'ANSSI et/ou au fournisseur de services dans certains cas[21].** En cas d'« impact significatif » sur le service fourni, une notification devra être formulée par le fournisseur de services à l'ANSSI en France, ou par l'opérateur de services essentiel impacté au fournisseur de services. La notification à l'ANSSI devra être formulée « sans retard injustifié ». Bien qu'aucune précision ne soit apportée dans la Directive sur la durée exacte acceptée pour la réception de cette notification, cette durée peut être comparée à celle de la notification adressée à la CNIL en cas d'atteinte au traitement de données à caractère personnel, qui est de 72h. Il semble donc que la notification adressée à l'ANSSI devra se faire dans un très court délai également. Cette notification devra de plus être formulée par courrier recommandé avec accusé de réception.

## Récapitulatif des obligations de notification :




**En conclusion,** la Directive NIS va conduire les entreprises, directement ou indirectement, à prendre des mesures en matière de sécurité informatique : évaluer les risques potentiels pouvant toucher leur système d'information et prendre les mesures de protection adéquates. L'accent est mis sur la prévention. Si malgré ces précautions les systèmes d'information sont atteints, la Directive NIS oblige également les entreprises à limiter les conséquences de cet impact et à le notifier au plus vite.

# RGPD
## Règlement Général sur la Protection des Données

**Au final, le RGPD et la Directive NIS adoptent une logique similaire quant à la cybersécurité :**

| Directive NIS | RGPD |
|---|---|
| **Protection des réseaux et des SI** | **Protection des données à caractère personnel** |
| **Mesures préventives techniques et organisationnelles** à adopter (identification des risques, mesures préventives, continuité du service). | **Mesures techniques et organisationnelles** à adopter (sécurisation du traitement de données, analyse d'impact, obligation de rendre des comptes). |
| **Notification** à l'ANSSI (ou CSRIT) en cas d'incident affectant la sécurité des réseaux ou des SI. | **Notification** à la CNIL en cas de faille de sécurité dans un délai maximum de 72h. |
| Pas de sanction prévue par la Directive NIS, mais le Code pénal français punit déjà pénalement les atteintes au SI. | Sanction administrative pouvant s'élever jusqu'à 20 000 000 € ou 4% du chiffre d'affaires annuel mondial total. |

**21.** Art. 16 (3) & art. 16 (5)

# Présentation de cas typiques d'actions relatives à la cybersécurité et pouvant impacter les organisations

Nous proposons la présentation d'une sélection de cas connus d'atteintes à des systèmes d'information, accompagnée de notre analyse.

## Cas n°1 : une faille de sécurité conduit à la fuite de plus d'un million de données à caractère personnel = avertissement public de la CNIL

**Les faits :** Le 7 août 2014, suite à une **faille de sécurité**, un avertissement public est prononcé à l'encontre d'ORANGE® par la CNIL pour manquement à son obligation de sécurité des données à caractère personnel[22]. La société sous-traitante d'ORANGE, victime d'une faille informatique, a subi la fuite de plus d'un million de données clients stockées. ORANGE a notifié la faille à la CNIL, qui a procédé à des contrôles auprès de cette dernière et de ses prestataires en charge de sa campagne d'emailing promotionnel. La CNIL a alors constaté l'existence de plusieurs manquements de la part d'ORANGE, responsable de traitement :

- ORANGE n'a pas réalisé d'audit de sécurité auprès de son prestataire pour l'envoi de campagnes d'emailing, alors que selon la CNIL cette mesure lui aurait permis de détecter la faille de sécurité et donc d'éviter la fuite des données personnelles.
- ORANGE n'a pas non plus pris soin de mettre en place des mesures de sécurité et de confidentialité lors de l'envoi de ses données clients à son entreprise prestataire, et n'a pas non plus imposé de clauses de sécurité et de confidentialité à ces dernières.

La CNIL a donc constaté qu'ORANGE avait manqué à son obligation d'assurer la sécurité et la confidentialité des données à caractère personnel que l'entreprise traite, selon l'article 34 de la loi « Informatique et Libertés ». S'en est suivi un **avertissement public** à l'encontre d'ORANGE.

**À retenir – risque juridique :** une entreprise gérant des données à caractère personnel devra prendre toutes les précautions utiles pour la confidentialité et la sécurité des données à caractère personnel qu'elle a collectées. À défaut, et bien que victime d'une cyberattaque comme dans le cas traité, elle pourra être responsable juridiquement.

### Avant de contracter avec ses sous-traitants

- Faire des audits de sécurité en amont.
- Signature d'accords de confidentialité et de sécurité.
- Insertion de clauses de contrat « type » spécifiques aux sous-traitants proposés par la CNIL.

### Lors de transfert de données au sous-traitant

- Mettre en place des mesures de sécurité et de confidentialité lors de l'envoi des données.

## Cas n°2 : Suite à une cyberattaque, les services sont suspendus pendant plusieurs jours

**Les faits :**

**Affaire n° 1 :** *Le 8 avril 2015, suite à une cyberattaque, FRANCE TV5 MONDE® voit ses programmes suspendus pendant deux jours.*

La chaîne de télévision FRANCE TV5 MONDE est victime d'une cyberattaque conduisant à la fermeture de ses programmes pendant deux jours et à la publication d'un message de soutien à l'État islamique sur les pages officielles de la chaîne, notamment sur ses réseaux sociaux. Outre les dommages matériels subis, cette cyberattaque a porté atteinte à l'image de la chaîne.

**Affaire n° 2 :** *Le 21 janvier 2012, VIVENDI® est victime de cyberattaques par le groupe Anonymous…*

En janvier 2012, le site du groupe VIVENDI a été attaqué par des membres de la mouvance Anonymous. Lors de cette attaque, le site a affiché pendant plusieurs minutes le logo du mouvement Anonymous, ainsi qu'un texte accusant le groupe VIVENDI entre autres *« d'actes de censure et de haute trahison envers l'esprit Internet »*. Mais surtout, les données des comptes de messagerie de plus de 800 personnes auraient été volées et auraient été mises à disposition en ligne. L'affaire n'a été jugée que le 6 novembre 2015 par le Tribunal correctionnel, soit plus de trois ans après l'attaque.

**À retenir – risques d'image et financier, risque juridique :** afin de se prémunir face à une attaque similaire, l'entreprise peut mettre en place plusieurs mesures :

1. Mobiliser les directions générales, techniques (DSI) de sécurité, de communication et juridique.
2. Initier sans délai une enquête interne sans destruction de preuves, faire appel à des experts, faire constater par des Huissiers de justice.
3. Signaler l'attaque aux autorités de police (Ministère de l'intérieur) en cas notamment de risque d'espionnage industriel ou de sabotage économique ou judiciaire si l'affaire est déjà dans le public. Dans ce dernier cas, le signalement prendra la forme d'une plainte pénale qui a pour fonction, notamment, de tenter d'élucider l'attaque.
4. Former ses personnels tout au long de l'année, prévoir un plan d'action.

## Cas n° 3 : les contrôles de la CNIL sont nombreux et précis

**Les faits :**

**Affaire n° 1 :** *Le 7 juillet 2016, sanction de la CNIL à l'encontre de la société BRANDALLEY® dans le cadre de contrôle.*

Après avoir effectué un premier contrôle en 2015, la CNIL constate que la société BRANDALLEY manque à ses obligations de responsable de traitement en termes de sécurité des données. Un an après, un second contrôle est effectué afin de vérifier si la société BRANDALLEY a pris en compte les remarques de la CNIL. Cette dernière a constaté la persistance des manquements à la loi « Informatique et Libertés » par la société, notamment :

- Manquement à l'obligation de définir et mettre en œuvre une durée de conservation des données (mesure préventive de protection).
- Manquement à l'obligation d'assurer la confidentialité et la sécurité des données : notamment l'absence de mise en œuvre d'un protocole « https » sécurisé sur le site qui ne permettait pas de garantir le « chiffrement du canal de communication et une authentification du site distant ».
- Manquement à obligation de respecter les règles relatives au transfert de données à caractère personnel hors Union européenne.

La CNIL a donc prononcé une sanction pécuniaire d'un montant de 30.000 euros à l'encontre de la société BRANDALLEY. Ainsi, outre les dommages matériels et l'atteinte à l'image que peuvent causer les carences en matière de cybersécurité, la CNIL peut également prononcer des sanctions assorties d'amendes administratives élevées.

**Affaire n° 2 :** *En juillet 2016, la CNIL met en demeure MICROSOFT® de rendre son système d'exploitation conforme à la loi « Informatique et Libertés ».*

La CNIL a mis en demeure MICROSOFT de rendre son système d'exploitation Windows® 10 conforme à la loi « Informatique et Libertés » en juillet 2016, et lui laisse 3 mois pour se conformer à sa décision. La CNIL reproche à MICROSOFT plusieurs manquements :

- MICROSOFT collecte un nombre excessif de données à caractère personnel.
- MICROSOFT manque à son obligation d'assurer la sécurité des données collectées.

> *« La société permet aux utilisateurs de choisir un code PIN de 4 chiffres pour s'authentifier pour l'ensemble de ses services en ligne et notamment pour l'accès à leur compte MICROSOFT, qui recense les achats effectués sur le store et les moyens de paiement utilisés. Or, le nombre de tentatives de saisie de ce code PIN n'est pas limité, ce qui n'assure pas la sécurité et la confidentialité des données des utilisateurs[23] ».*
>
> **Extrait décision CNIL**

**À retenir – risques juridiques :**

1. Même en l'absence de fraude informatique ou cyberattaques, la CNIL peut prononcer des sanctions à l'encontre des entreprises responsables de traitement.

2. Les sanctions peuvent être et sont de plus en plus publiques. Ces sanctions, outre leur éventuel coût, portent atteinte à l'image de l'entreprise.

## L'analyse de ces différents cas conduit aux conclusions suivantes :

- Une cyberattaque passe rarement inaperçue…le préjudice d'image est non négligeable pour l'entreprise victime.
- L'ampleur des préjudices (atteinte à l'image, vol de données…).
- La réponse des institutions judiciaires est longue.
- Les sanctions sont lourdes pour les entreprises qui ne sécurisent pas leurs systèmes d'information.
- La prévention technique des systèmes d'information reste donc la première réponse et est primordiale.

**23.** www.cnil.fr/fr/windows-10-la-cnil-met-publiquement-en-demeure-microsoft-corporation-de-se-conformer-dans-un-delai

# Pourquoi la technique est-elle la première réponse ?

Aujourd'hui, les entreprises en charge de systèmes d'information doivent favoriser la technique comme première réponse face à d'éventuelles cyberattaques, et cela pour plusieurs raisons :

- **La technique fait désormais partie des obligations légales :** imposée tant par le RGPD que dans la Directive NIS, ces deux textes préconisent la mise en place de plusieurs mesures techniques de protection dès la conception du système d'information (« Privacy by Design »).
- **L'expérience a démontré qu'à ce jour la technique est la meilleure solution pour faire face à la cybercriminalité.** Les affaires citées ci-dessus révèlent toutes que c'est l'absence ou la mauvaise gestion des techniques de protection qui a engendré les cyberattaques.
- **La technique apparaît donc comme la première des garanties en matière de cybersécurité pour l'entreprise.**

Les deux techniques de protection les plus abouties et reconnues comme telles par l'analyse des cas et par les deux autorités en charge de la sécurisation des SI (CNIL et ANSSI) sont l'authentification et la cryptologie.

## L'authentification : mise en œuvre et mise à jour

L'authentification est définie par l'ANSSI comme une technique qui « a pour but de vérifier l'identité dont une entité se réclame » [24].

L'utilité et la nécessité de l'authentification s'apprécient à deux niveaux :

- L'authentification permet de protéger les systèmes d'information contre toute intrusion ou tout acte illicite.
- L'authentification permet également de savoir précisément qui a eu accès au système d'information et d'en conserver la preuve.

### Les questions préalables

#### Qu'est-ce qui nécessite un accès protégé ?

Tout matériel ou interface dont le contenu ou la structure nécessite d'être protégé, notamment :

- Les systèmes d'information (*comprenant des authentifications allant de simples à fortes*).
- Les ordinateurs.
- Le WiFi.
- Les téléphones portables (*généralement un mot de passe numérique*).
- Les objets connectés (*développement d'une authentification biométrique*).

## Les précautions à prendre concernant l'accès au WiFi :

dans un arrêt récent rendu par la Cour de Justice de l'Union européenne du 15 septembre 2016, cette dernière a considéré que celui qui propose au public et gratuitement un accès au WiFi peut se voir enjoindre de sécuriser la connexion par un mot de passe. Cet arrêt illustre bien la préoccupation actuelle de sécurisation des systèmes d'information, et rappelle que le WiFi reste un protocole de communication risqué s'il n'est pas protégé.

Dans son guide des bonnes pratiques, l'ANSSI déconseille aux entreprises d'accéder à Internet par un point d'accès WiFi, et de privilégier une installation filaire. Si le WiFi est le seul moyen pour accéder à Internet, des précautions particulières doivent être prises.

### Les personnes bénéficiant de l'authentification / des différents niveaux de sécurité

**Les responsables des systèmes d'information, des traitements de données à caractère personnel et leurs sous-traitants** doivent s'assurer que l'accès à leur système d'information est restreint et n'est autorisé qu'aux personnes habilitées. La technique de l'authentification permet de vérifier l'identité de la personne qui souhaite accéder au système d'information.

**Il existe différents niveaux de sécurité pour l'authentification :**

- Il existe ainsi trois catégories de niveau d'authentification des personnes :
  - un élément que seul l'utilisateur connait comme le mot de passe
  - un élément que seul l'utilisateur détient comme une carte à puce
  - un élément propre à l'utilisateur comme ses données biométriques (son empreinte digitale, sa signature...)
- À partir de ces catégories, l'authentification sera jugée :
  - simple si l'authentification ne repose que sur une seule de ces catégories
  - forte si l'authentification repose sur au moins deux de ces catégories (selon la CNIL[25])

L'authentification recouvre deux notions : l'utilisation d'une technique fiable et la mise en œuvre de procédure interne afin de garantir son efficacité.

**24.** ANSSI, « Glossaire de la sécurité informatique », www.cil.cnrs.fr/CIL/IMG/pdf/Glossaire_securite_informatique.pdf
**25.** CNIL, « Sécurité des données personnelles », p.9

### 1. Une technique fiable

L'authentification est considérée comme une technique fiable par la CNIL et l'ANSSI :

| CNIL | ANSSI |
|---|---|
| **Un identifiant unique par utilisateur est recommandé.** | **Aucun accès anonyme au réseau ne doit être autorisé : il faut identifier strictement qui peut avoir accès aux fichiers.** |
| **Authentification par mot de passe**<br>▶ Il doit comporter 8 caractères minimum de 3 types différents (chiffres, majuscules, minuscules, caractères spéciaux).<br>▶ Son renouvellement doit être fréquent.<br>▶ Le mot de passe par défaut doit être modifié par l'utilisateur.<br>▶ Il ne faut pas utiliser un même compte pour plusieurs usagers. | **Authentification par mot de passe**<br>▶ Il est recommandé de le composer de 12 caractères minimum.<br>▶ Il ne doit pas être lié à l'identité de l'utilisateur.<br>▶ Son renouvellement doit être fréquent.<br>▶ Configurer les logiciels pour qu'ils n'enregistrent pas automatiquement les mots de passe. |
| **Authentification par des dispositifs biométriques :** une demande d'autorisation auprès de la CNIL est nécessaire[26]. | **Modifier systématiquement les éléments d'authentification par défaut** des équipements et services[27]. |
| **Mise en place d'une procédure de gestion des habilitations :** mise à jour régulière des profils d'utilisateurs qui ont le droit d'accéder ou non à certains types de données, suppression des permissions d'accès des utilisateurs qui ne sont plus habilités à accéder aux données. | **Afin d'assurer la sécurité du processus d'authentification, mise en place d'éléments temporaires :** l'effacement des données doit être un automatisme lorsqu'elles ne sont plus utiles. |
| **En cas d'accès à des données sensibles, des moyens d'authentification forte doivent être utilisés, notamment pour : notamment pour les données de santé et bancaires.** | **Authentification forte à privilégier pour les entreprises** (par exemple par carte à puce ou signature électronique).<br>▶ **Séparer usage personnel et professionnel :**<br>• Pas d'hébergement de données professionnelles sur des appareils ou sites d'hébergement personnels.<br>• Les mails professionnels ne doivent pas être transférés sur une messagerie personnelle. |

**À noter : ces recommandations peuvent être cumulatives.**

**Parmi les techniques d'authentification, la signature électronique et l'horodatage électronique** sont mentionnés dans le nouveau règlement 910/2014 dit « eIDAS », applicable depuis le 1er juillet 2016.

**Ces deux moyens d'authentification se distinguent par le fait qu'ils permettent de fournir une preuve fiable et surtout de renverser la charge de la preuve au bénéfice de celui qui les instaure.**[28]

**La signature électronique**

- Permet l'authentification d'une personne souhaitant accéder à un système d'information.
- Défini comme : « *une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification*».
- Il y a plusieurs types de signatures électroniques, dont la signature électronique avancée et qualifiée. Seule la signature électronique dite « qualifiée » a la même valeur que la signature manuscrite.

**L'horodatage électronique**

- Permet d'authentifier un acte et de prouver l'exactitude de sa date.
- Défini comme « *des données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant*».
- Il y a plusieurs niveaux de garantie d'horodatage électronique. L'horodatage électronique « qualifié », niveau le plus élevé, doit satisfaire aux conditions de l'art. 41 du règlement 910/2014.

La technique ne peut être efficace que si une organisation en interne est instaurée par l'entreprise.

**26.** www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/Communication-biometrie.pdf
**27.** www.ssi.gouv.fr/uploads/IMG/pdf/pssie_anssi.pdf
**28.** Art. 25 al.2 règlement 97/2014 : « L'effet juridique d'une signature électronique qualifiée est équivalent à celui d'une signature manuscrite. »

## 2. La mise en œuvre d'une procédure interne afin de garantir son efficacité

L'entreprise doit s'assurer que ses données sont traitées dans un environnement hautement sécurisé, avec :

1. **La mise en place de structures de qualité et d'habitude «sécurisée»** : accès fermé, mot de passe sur les ordinateurs...

2. **Définir les droits d'accès :** la CNIL recommande de mettre en place des profils d'habilitation afin de déterminer quel utilisateur peut accéder à quel type de données (CNIL, Fiche n°10 « Sécurité des données »).

3. **Sensibiliser les utilisateurs et notamment les salariés au processus d'authentification à travers des documents non contractuels** (règles de sécurités, Charte informatique) **mais surtout des documents contractuels** (Charte annexée au règlement intérieur, insertion d'une clause dans le contrat de travail...).

Bien que l'authentification soit une technique fiable et reconnue, le chiffrement est une technique présentant des moyens de protection supérieurs.

## La cryptologie

**Art. 29 LCEN :**

*« On entend par moyen de cryptologie tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète.* ***Ces moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité.*** *»*

### Pourquoi la cryptologie est-elle aujourd'hui nécessaire ?

La cryptologie est l'une des techniques les plus fiables pour sécuriser le système d'information d'une entreprise. Il s'agit d'une technique qui permet de chiffrer un message afin de le rendre lisible uniquement par son destinataire, qui détient la clé de décodage.

Cette technique permet d'assurer :

- La confidentialité des données (qui ne peuvent être lu par personne d'autre que le destinataire).
- Leur authentification (seule la personne qui détient la clé de décodage est identifiée comme destinataire légitime des données chiffrées).
- Le contrôle de leur intégrité (grâce à cette méthode, les données ne sont ni détruites, ni altérées, ni volées).

**Illustration de l'importance prise par la cryptologie :**

**En octobre 2016, la CNIL prononce un avertissement public et met en demeure C-Discount notamment pour « défaut de sécurité »**

La CNIL considère que la Société C-DISCOUNT® *« n'a pas mis en œuvre de moyens suffisants pour assurer la sécurité et la confidentialité des données personnelles de ses* ***clients en conservant en clair*** *dans un champ commentaire de sa base de données, lesdits numéros des cartes bancaires »*[29].

## Le régime spécial de la cryptologie

En France, les moyens de cryptologie sont soumis à une réglementation spécifique prévue par la loi pour la confiance dans l'économie numérique, dite « LCEN »[30].

**Il convient de rappeler tout d'abord que l'utilisation des moyens de cryptologie est libre, toute entreprise peut y avoir recours à tout moment sans accomplir aucune démarche.**[31]

**Article 30 de la loi LCEN :**

**I. – « L'utilisation des moyens de cryptologie est libre ».**

En revanche, la loi impose aux sociétés qui fournissent les moyens de cryptologie (création, fourniture, importation, création) des déclarations et autorisations préalables auprès des autorités compétentes (ANSSI et Premier ministre).

Ces démarches doivent être effectuées par le **fournisseur du moyen de cryptologie.**

**Il est donc recommandé de demander les justificatifs de ces démarches lorsqu'une entreprise a recours à ces services.**

**29.** www.cnil.fr/fr/cdiscount-avertissement-et-mise-en-demeure-pour-de-nombreux-manquements
**30.** Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique
**31.** Art. 30 loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (loi « LCEN »)

**Arrêté du 15 du 29 janvier 2015 définissant la forme et le contenu des dossiers de déclaration et de demande d'autorisation d'opérations relatives aux moyens et aux prestations de cryptologie.**

Fournit en annexe le formulaire de demande déclaration ou d'autorisation préalable à remplir.

## Formalités spécifiques pour l'exportation d'un moyen de cryptologie depuis la France :

Le fournisseur du moyen de cryptologie a dans ce cas deux démarches distinctes à effectuer :

- Formuler une demande d'autorisation ou de déclaration préalable auprès de l'ANSSI.
- Adresser une demande de licence auprès du service des biens à double usage (SBDU) en y joignant une copie des documents délivrés par l'ANSSI.

**Deux types de sanctions encourues en cas de non-respect des formalités :**

- **Sanction administrative** (art. 34 loi LCEN) : interdiction de mise en circulation (art. 34 de la loi LCEN).
- **Sanctions pénales** (art. 35 loi LCEN) :
  - jusqu'à un 1 an d'emprisonnement et 15.000 euros d'amende en cas de manquement à l'obligation de déclaration ou de communication au Premier ministre
  - jusqu'à deux 2 ans d'emprisonnement et 30.000 euros d'amende en cas de manquement à l'obligation de demande d'autorisation
  - peines complémentaires : confiscation, fermeture d'établissement, exclusion des marchés publics

**À noter :** l'ANSSI délivre des attestations de qualification aux techniques de protection des systèmes d'information, permettant aux entreprises de confier sa protection à des prestataires de services labellisés.

**En conclusion**, la cybersécurité n'est plus seulement la protection du système d'information.

Elle est aussi la protection du maître du système d'information contre sa propre responsabilité juridique. Car on peut désormais être victime et responsable.

Internet, ce réseau de tous les réseaux, nous a rendus responsables les uns des autres. Aussi, les défaillances des uns peuvent avoir des conséquences pour les autres.

**L'année 2016 vient consacrer cette évolution.**

- Le système d'information est attaqué, des données à caractère personnel sont extraites de manière illicite, le responsable du système doit notifier cet évènement à la CNIL, éventuellement aux personnes concernées, sous peine de sanctions. C'est le RGPD qui rend cette mesure obligatoire pour tous dès le 25 mai 2018.
- Votre entreprise travaille dans des secteurs d'importance pour la stabilité des États et de leur population. En tant qu'opérateur dit de services essentiels, la loi vous impose des obligations particulières. C'est la Directive NIS qui doit être transposée au plus tard en mai 2018 par chaque État membre de l'Union européenne.
- Enfin, la loi française pour une république numérique du 7 octobre 2016 crée un statut protecteur pour les hackers blancs, ces personnes qui, de bonne foi, constatent une défaillance dans un système d'information. Ils peuvent désormais s'adresser à l'ANSSI pour signaler cette défaillance, et l'Agence conservera confidentiels leur identité et le moyen qu'ils ont utilisés pour découvrir cette vulnérabilité.

On le voit au travers de ces quelques exemples, plus que jamais, la loi européenne et française vient exiger de chacun qu'il connaisse ses droits, mais également ses devoirs en matière de cybersécurité.

Ce livre blanc vient ici, contribuer à cette exigence.

## Livres blancs

La sécurité informatique est un domaine ultra sensible qu'il faut absolument prendre en compte dans les entreprises. **La compréhension préalable des différentes menaces et tendances** aussi bien que **l'impact des solutions de sécurité informatique** devient primordial pour **établir une politique de sécurité efficace**. N'hésitez pas à télécharger et consulter régulièrement nos nouveaux livres blancs.


- Règlement Général sur la Protection des Données et le Safe Harbor 2
- Évolution des logiciels malveillants hors de l'écosystème Windows
- Comment contrer efficacement les ransomwares ?
- Sécuriser les environnements virtuels
- Internet des objets : quelle sécurité pour les milliards d'objets connectés utilisés par les entreprises ?

**www.eset.com/fr/livres_blancs**

ENJOY SAFER TECHNOLOGY™*

## CONTACTEZ-NOUS

ESET France

Tel. + 33 (0)1.55.89.08.85

www.eset.com/fr

www.welivesecurity.com