Entreprises et cyberattaques

Cybersécurité et réponses juridiques

Myriam Quéméner, magistrat honoraire , docteur en droit

Panorama de la cybermenace de l'ANSSI

Panorama Cybermenace 2025

ANSSI - Analyse France

29% 0
Vulnérabilités exploitées en J-0
Exploitation le jour même ou avant publication officielle

+51%
Exfiltrations de données
Priorité au vol sur le simple chiffrement (196 cas)

-9%
Attaques par rançongiciels
Légère baisse (128 cas), mais menace majeure pour PME/santé

1 366
incidents confirmés
Volume stable, sophistication accrue des modes opératoires

Secteurs sous Haute Pression

76% des incidents concentrés sur ces 4 secteurs clés :

- **Éducation et Recherche (34%)** — Souvent systèmes peu sécurisés
- **Administrations et Collectivités (24%)** — Ciblage constant des institutions
- **Santé (10%)** — Impact vital sur la continuité de service
- **Télécoms (9%)** — Impact vital sur la continuité de service

Évolutions et Modes Opératoires

- **Exfiltration prime sur le chiffrement** — Chantage à la divulgation
- **Hybridation des attaquants** — Confusion acteurs étatiques/cybercriminels
- **Exploitation ultra-rapide des failles** — Délai d'exploitation réduit à quelques heures

Menaces et Acteurs Marquants

- **Souches dominantes :** Qilin (21%), Akira (9%)
- **Équipements de bordure ciblés :** Ivanti, Fortinet, SharePoint
- **Acteurs étatiques :** APT28 (Russie), Salt Typhoon (Chine), Moonstone Sleet (Corée du Nord)

⚠ Cas de Rupture et Actions 2026

- **Sabotage coordonné**
- **Compromission de la BITD**
- **Actions prioritaires 2026** — Sécuriser la supply chain, Patcher failles critiques en <48h, Assurer conformité NIS2 et CRA

NotebookLM


ALERTE INFO
Fuites de données : un homme de 22 ans, surnommé "HexDex", placé en garde à vue après de nombreuses cyberattaques contre des fédérations sportives, syndicats et administrations

Les infractions dites classiques

- Vols , collectes illégales de données
- Escroqueries (répression du phishing)
- Extorsions
- Association de malfaiteurs
- Contrefaçon

La loi du 13 novembre 2014: la reconnaissance du vol de données par le biais de l'extraction

En matière pénale, afin de prendre en compte les évolutions technologiques, la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme a incriminé le « vol » de données et a créé l'infraction d'atteinte à un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État commise en bande organisée.

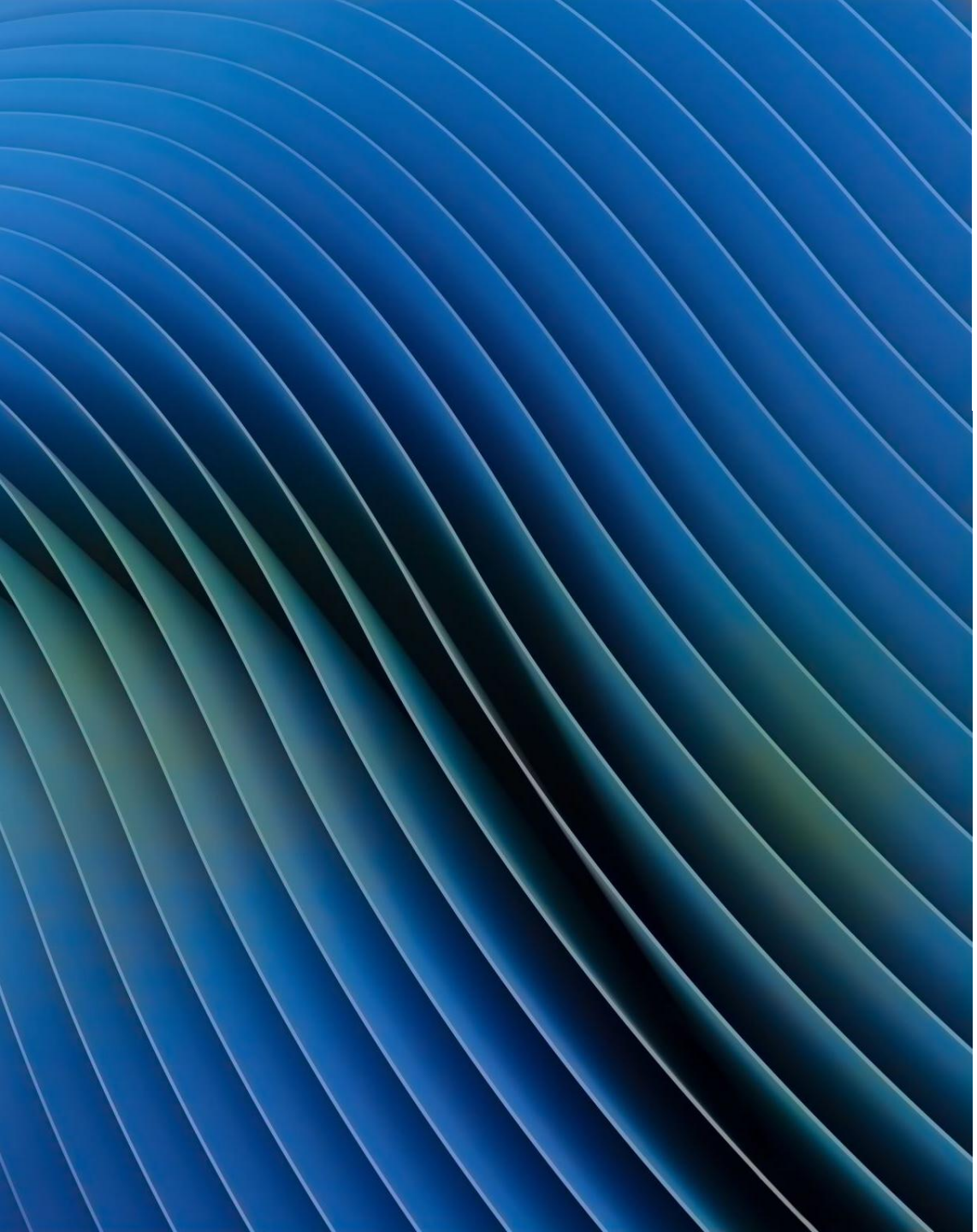
La loi du 24 juillet 2015 relative au renseignement a par ailleurs rehaussé les peines pour les différentes atteintes à un système de traitement automatisé e données.

Les infractions réprimant les modes opératoires des fraudes numériques

Accès et maintien frauduleux dans un STAD : 3 ans et 100 000 euros (Art. 323-1 du CP)

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, 5 ans et 150 000 euros.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à 7 ans et 300 000 euros d'amende.



Autres atteintes aux STAD

Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de *5* ans *et de* 150 000 €» d'amende.(Art 323-2 du CP).

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à 7 ans et à 300 000 € d'amende.

Le fait d'introduire frauduleusement des données dans un système de traitement automatisé *(L. nº 2014-1353 du 13 nov. 2014, art. 16)* «, d'**extraire**, de détenir, de reproduire, de transmettre,» de supprimer ou de modifier frauduleusement les données qu'il contient est puni de *(L. nº 2004-575 du 21 juin 2004, art. 45-III)* «cinq ans» d'emprisonnement et de *(L. nº 2015-912 du 24 juill. 2015, art. 4)* «150 000 €» d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à sept ans d'emprisonnement et à *(L. nº 2015-912 du 24 juill. 2015, art. 4)* «300 000 €» d'amende.»

Les délits d'atteintes aux systèmes d'information

L'accès ou maintien dans un STAD

- Puni par l'article 323-1 du code pénal **de 3 ans d'emprisonnement** et de **100 000€ d'amende.**
- Lorsque commis à l'encontre d'un STAD mis en œuvre par l'Etat : **7 ans d'emprisonnement** et **300 000€ d'amende**.

Entraver ou fausser le fonctionnement d'un STAD

- Sanctionné par l'article 323-2 du code pénal de 5 ans d'emprisonnement et 150 000€ d'amende.
- Lorsque commis à l'encontre d'un STAD mis en œuvre par l'Etat: 7 ans d'emprisonnement et 300 000€ d'amende.

Modification frauduleuse de données dans un STAD

- Introduction, extraction, détention, reproduction, transmission, suppression ou modification frauduleuse des données
- Punies par l'article 323-3 du code pénal de **5 ans d'emprisonnement** et **150 000€ d'amende**.
- Lorsque commis à l'encontre d'un STAD mis en œuvre par l'Etat: 7 ans d'emprisonnement et 300 000€ d'amende.

Instrument ou programme informatique pour commettre une infraction

- Importer, détenir, offrir, céder ou mettre à disposition
- Punis par l'article 323-3-1 du code pénal des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Effet exposant autrui à un risque immédiat de mort ou de blessures

- Puni par l'article 323-4-2 du code pénal de **10 ans d'emprisonnement** et **300 000 € d'amende.**

L'ARSENAL JURIDIQUE FACE AUX CYBERATTAQUES

Atteintes aux systèmes 323-1 et ss CP
(accès et maintien frauduleux dans un STAD; entrave 323-2 cp par déni de service)
Extraction de données 323-3 CP
Atteintes aux données (**cf.** accès et maintien frauduleux dans un STAD avec influence sur les données; défigurations de sites)

-

- **Contrefaçon** de marques D,B M du CPI
- Contrefaçon d'œuvres téléchargement illégal film musique (même liens vers torrents)
- Liens commerciaux et cybersquatting

Infractions traditionnelles:
Vol 311-1 CP
Escroquerie 313-1
Abus de confiance 314-1
Extorsion 312-1

323-3-2 CP
Administration illicite de plate-forme en ligne

-18 du CP
ecte de données à l'insu des personnes
- Spamming/ SPhishing / Smishing
441-1 et ss
Usurpation d'identité / de titre
226-4-1 CP
Usurpation de données de toute nature telle l'identité
- **226-8 Usage DEEP FAKE diffusion montage ou image sans consentement (Loi 21-5-24)**
226-8-1 diffusion de paroles et image reproduites
- **par IA**
Sextorsion 227-22-2

Administration d'une plate forme permettant une transaction illicite (323-3-2°)

Circonstance aggravante de bande organisée

Absence de motif légitime

- Le fait, sans motif légitime notamment de recherche ou de sécurité informatique», d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Délit d'administration illicite d'une plateforme en ligne (Art.323-3-2 du CP)

Le fait pour une personne qui fournit un service de plateforme en ligne **de, sciemment, permettre** la cession de produits, de contenus ou de services, dont la cession, l'offre, l'acquisition ou la détention sont **manifestement illicites**, et, pour cela :

- – soit restreindre l'accès à ce service aux personnes utilisant des techniques d'anonymisation des connexions ;
- – soit ne détenir, ni ne conserver les données d'identification de ses utilisateurs

- pour tout individu de proposer, par l'intermédiaire d'un fournisseur de service de plateforme en ligne, des prestations d'intermédiation ou de séquestre qui ont pour objet unique ou principal de mettre en œuvre, de dissimuler ou de faciliter les opérations de cession de ces produits, contenus ou services.

Les peines prévues sont de cinq d'emprisonnement et de 150 000 euros d'amende, et passent à dix ans d'emprisonnement et 500 000 euros d'amende lorsque ces infractions sont commises en bande organisée.

Répression des fraudes numériques

Généralement , les deux types d'infractions sont retenus (Modes opératoires visant un STAD et infractions classiques souvent aggravées par la circonstance de bande organisée)

Investigations grâce à des procédures adaptées au numérique (Réquisitions, , captations de données , enquêtes sous pseudonyme avec recours à l'IA

Répression des deepfakes

L'article 226-8 du code pénal punissait d'un an d'emprisonnement et de 15 000 euros d'amende le fait de « *publier, par quelque voie que ce soit, le montage réalisé avec les paroles ou l'image d'une personne sans son consentement, s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention* ».

Avec la loi LSREN, il est aussi interdit de « *porter à la connaissance du public ou d'un tiers, par quelque voie que ce soit, un contenu visuel ou sonore généré par un traitement algorithmique et représentant l'image ou les paroles d'une personne, sans son consentement, s'il n'apparait pas à l'évidence qu'il s'agit d'un contenu généré algorithmiquement ou s'il n'en est pas expressément fait mention* ».

La commission de ce délit sur les réseaux sociaux devient une circonstance aggravante augmentant les peines à deux ans d'emprisonnement et 45.000€ d'amende.

retrait Blocage des sites illicites

- La loi du 13 novembre 2014 relative à la lutte contre le terrorisme permet le **blocage** par l'autorité **administrative des sites Internet** provoquant à des actes de terrorisme ou en faisant l'apologie ainsi que des **sites** contenant des représentations de mineurs à caractère pornographique.

LE DROIT PROCESSUEL LA RECHERCHE DE LA PREUVE

:

LES PRINCIPES DE LA COLLECTE DE LA PREUVE NUMÉRIQUE

LES PROCÉDURES D’ENQUETES

LES TECHNIQUES D’ENQUETE

LA COOPERATION INTERNATIONALE

LES PRINCIPES :

La preuve est recueillie selon **les principes fondamentaux du droit et des libertés fondamentales** dans le souci de **l'équilibre entre les exigences de la sécurité publique des biens et des personnes et celle de la protection de la liberté individuelle**.

La provocation à la preuve est possible mais non à l'infraction

- **Cf. les techniques d'enquêtes.**

Une collecte des éléments de preuve: **loyale, proportionnée et nécessaire aux besoins** de l'enquête et soumise au **contradictoire**. (Pas de stratagème ni d'artifice pour l'enquêteur mais possible pour la victime)

CADRES JURIDIQUES D'ENQUETE

- LA FLAGRANCE 53 et ss CPP motu proprio

- PRELIMINAIRE 75 et ss CPP Instructions et d'office

- RECHERCHE DES CAUSES DE LA MORT ou DECOUVERTE D'UNE PERSONNE GRIEVEMENT BLESSEE 74 CPP

  - DISPARITIONS INQUIETANTES 74-1 CPP
  - PERSONNES EN FUITE 74-2 CPP

- L'INFORMATION 79 et ss CPP

  - La commission rogatoire 81 et 151et ss

Moyens classiques de recueil des éléments dans les procédures d'enquête:

Les constatations des faits techniques (sur remises et/ou saisies)

Les réquisitions aux personnes (mails et réponse dans des formats informatiques exploitables 60-1, 77-1-1 et accord si 56-1 à 56-5 CPP)

Les perquisitions 56 CPP chez le titulaire de l'abonnement IP ou ligne téléphonique (75 CPP EP)

Procédures

Enquête sous pseudo

Captations de données

Accès à distance

Recours à l’IMSI Catcher

Apport de la loi narco

Les enquêteurs habilités agissant sous pseudonyme (CPP, art. 230-46) ou en infiltration (CPP, art. 706-81), pourront recourir à des « dispositifs » techniques ayant pour objet ou pour effet « d'altérer ou de transformer leur voix ou leur apparence physique » (adde, C. douanes, art. 67 bis, II, 67 bis-1 A, 1° et 67 bis-1, 3°).

Elle est un pouvoir conféré aux enquêteurs pour masquer leur identité réelle : le deepfake – ou hypertrucage – n'est plus l'apanage des délinquants (C. pén., art. 226-8 et 226-8-1) ; il est aussi une technique d'enquête visant à garantir l'anonymat des enquêteurs tant à des fins probatoires qu'à des fins de protection. "

Compétence territoriale

En matière de crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale a créé un **nouvel article 113-2-1** dans le Code pénal qui dispose : « Tout crime ou tout délit réalisé au moyen d'un réseau de communication électronique, lorsqu'il est tenté ou commis au préjudice d'une **personne physique résidant sur le territoire de la République ou d'une personne morale dont le siège se situe sur le territoire de la République**, est réputé commis sur le territoire de la République ».

Le législateur privilégie le domicile de la victime personne physique ou le siège social de la personne morale pour retenir la compétence.

Tribunal judiciaire de Paris et cybercriminalité (section J3)

La loi n° 2016-731 du 3 juin 2016 a renforcé les dispositions du titre XXIV du livre IV du Code de procédure pénale.

L'article 706-72-1 du Code de procédure pénale confie ainsi au procureur de la République de Paris, au pôle de l'instruction, au tribunal judiciaire et à la cour d'assises de Paris une compétence concurrente nationale en matière d'atteintes aux STAD et d'atteintes aux intérêts fondamentaux de la nation (cybersabotage), pour les affaires complexes et étendues géographiquement.

La saisine du parquet et du tribunal judiciaire de Paris, fondée sur la compétence nationale concurrente pour les infractions relatives aux STAD, ne relève pas d'une initiative de la partie civile, mais uniquement de celle du parquet d'un autre tribunal territorialement compétent qui requerrait le dessaisissement au profit de la juridiction parisienne. Cette spécialisation a été confortée par la loi n° 2019-222 du 23 mars 2019 qui a créé une nouvelle compétence au profit du tribunal judiciaire de Paris qui est devenu la juridiction nationale chargée de la lutte contre la criminalité organisée (JUNALCO).

Elle rassemble des magistrats spécialisés, chargés de conduire des enquêtes de grande ampleur, avec des investigations à l'échelle nationale ou internationale.

Rançongiciel : comment protéger votre organisation ?

Rançongiciel ou ransomware : que faire si votre organisation est victime d'une attaque ?

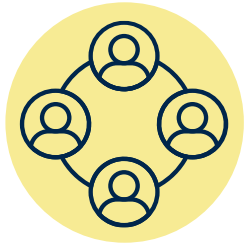
Réalisez des sauvegardes régulières de vos données, systèmes et applications critiques, en gardant des copies déconnectées, et en vérifiant périodiquement le bon fonctionnement de leur restauration.

Utilisez un pare-feu pour protéger les accès extérieurs à votre réseau informatique interne

Appliquez de manière régulière et systématique les mises à jour de sécurité.

Sécurisez les accès distants à votre réseau informatique interne en utilisant un VPN et systématisez l'emploi d'une double authentification

Utilisez une solution de protection contre les programmes et comportements malveillants (antivirus, EDR, XDR, ...)



Limitez les droits de tous les utilisateurs selon le "principe de moindre privilège".
Les collaborateurs doivent disposer uniquement des droits et accès strictement nécessaires pour l'accomplissement de leurs tâches.

Rançongiciel : comment protéger votre organisation ?

Rançongiciel ou ransomware : que faire si votre organisation est victime d'une attaque ?

Utilisez des mots de passe suffisamment longs, complexes et différents pour chaque service.

Supervisez la sécurité de votre système d'information.

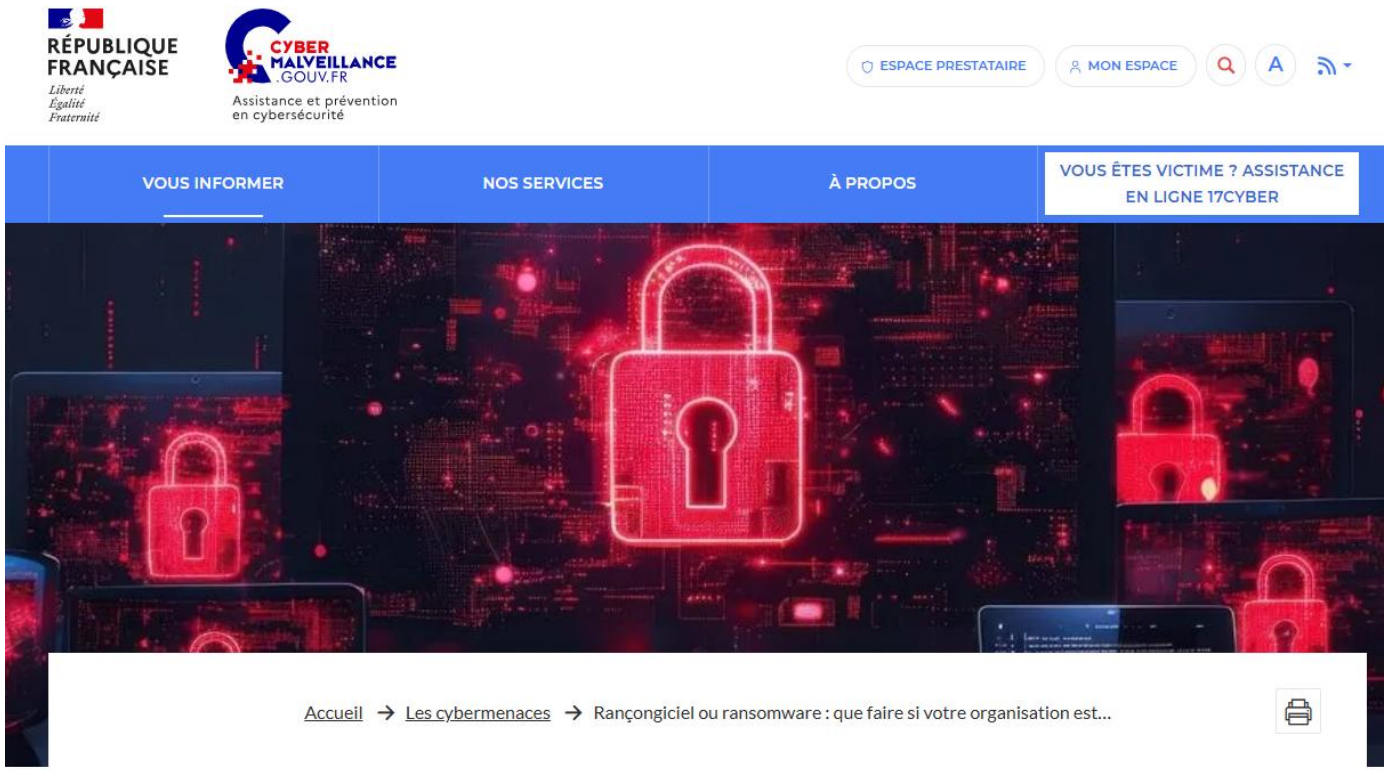
N'installez pas d'applications ou de logiciels "piratés".

Renforcez la sécurité de vos interconnexions à internet.

Sensibilisez l'ensemble de vos collaborateurs aux risques et rappelez régulièrement les consignes de sécurité.

Segmentez votre réseau informatique.

Le rançongiciel (ou ransomware)



Rançongiciel ou ransomware : que faire si votre organisation est victime d'une attaque ?

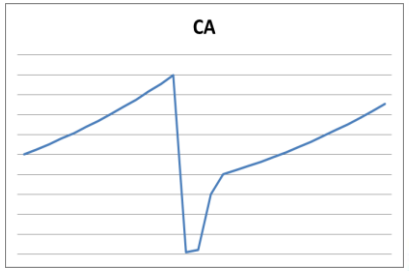
Payer ou ne pas payer ?

Gestion de crise

26

Ne pas payer ?

Impact sur l'activité	Surcoûts	Réclamation



Payer ?

« **Que faire en cas de ransomware** ? Isoler les équipements touchés, ne pas payer la rançon, préserver les preuves, identifier l'origine, déposer plainte… »

Se faire indemniser ?

Assurances:

A compter du 24 avril 2023, la loi d'orientation et de programmation du ministère de l'Intérieur (**LOPMI**) impose aux entreprises victimes d'atteintes informatiques malveillantes une **obligation de dépôt de plainte « au plus tard soixante-douze heures après la connaissance de l'atteinte par la victime » pour préserver leur droit à l'indemnisation au titre de leur contrat d'assurance** (L.12-10-1 du Code des assurances).

Déposer plainte auprès du Procureur de la République

Lorsque vous êtes victime d'une cyberattaque la plainte peut être déposée directement auprès du **Procureur de la République** par courrier recommandé.

Cette démarche est régie par **l'article 40-1 du Code de procédure pénale** qui assure que toute plainte sera examinée par l'autorité judiciaire compétente.

Seul le dirigeant représentant de la personne morale ou une personne ayant une délégation de pouvoir à cet effet, peut déposer plainte au nom de la personne morale.

Avantages

- **Protection des intérêts de votre entreprise**, vous avez la qualité de **victime**.
- En se constituant partie civile, vous pouvez demander des **dommages et intérêts** si l'affaire aboutit à un procès.
- Le dépôt de plainte peut être l'occasion pour l'entreprise de se faire **accompagner** par un avocat, permettant ainsi une meilleure **qualification juridique** des faits et une présentation claire de l'infraction au Procureur et un suivi de la procédure.

Contacter le 17Cyber

La **Police nationale**, la **Gendarmerie nationale** et **Cybermalveillance.gouv.fr** s'associent et lancent conjointement le site **17Cyber** : **équivalent numérique de l'appel 17**, destiné à toutes les victimes d'infractions numériques (particuliers, entreprises et collectivités).

Disponible 24h/24 et 7j/7, ce guichet unique permet aux victimes de comprendre rapidement, en répondant à quelques questions, à **quel type de menace** ils sont confrontés et ainsi, recevoir des **conseils personnalisés** en fonction de l'atteinte subie.

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

Gendarmerie nationale

POLICE NATIONALE

17 CYBER
Mon assistance en ligne

L'indemnisation des préjudices en cas d'infraction aux STAD*

➢ Les pièces à fournir à l'appui d'une demande d'indemnisation des préjudices matériels

*STAD : système de traitement automatisé des données

1

Frais d'assistance et d'expertises engagés à l'occasion de la crise :

➔**Typologie :** frais d'avocats, frais d'expertises (recherche de preuves techniques, restauration des données, etc.), accompagnement pour la communication de crise, frais d'huissiers, etc.

2

Frais relatifs à l'éventuelle communication à destination des personnes concernées :

➔**Typologie :** Frais d'envoi de mails, de courriers, de création d'un message d'alerte sur le site web etc.

3

Frais engagés par la gestion interne de la crise :

➔**Typologie :** temps passé par les équipes internes mobilisées (heures supplémentaires, astreintes, etc.).

➔**Pièces justificatives à produire :** factures, relevé de compte attestant du paiement des factures, journal des achats attestant de l'acquittement des factures.

Quelle responsabilité pour :

Le dirigeant ?

Focus sur la responsabilité pénale : Les effets de la délégation de pouvoir

Principe

Un employeur peut s'exonérer de sa responsabilité pénale s'il rapporte la preuve qu'il a délégué ses pouvoirs à une personne pourvue de la **compétence**, **l'autorité** et les **moyens nécessaires** pour assurer sa mission.

➔ A défaut de réunir ces **trois conditions cumulatives**, la délégation de pouvoirs n'est pas valable (Cass. crim., 6 janv. 2004, n° 02-87518 - Cass. crim., 8 déc. 2009, n° 09-82183).

Point de vigilance : le transfert de responsabilités ne s'effectue que dans les domaines visés par la délégation de pouvoir.

Quelques bonnes pratiques…

Pour se protéger personnellement

- Mettre en place des **délégations de pouvoirs** et de responsabilité pénale
  - vérifier la compétence de l'autorité effective du délégataire
  - rédiger une délégation expresse, précise et limitée
  - assurer au délégataire les moyens nécessaires pour accomplir sa mission

- Souscrire une **assurance** couvrant les risques de cybersécurité

- S'assurer de la **prise en compte du risque cyber** au plus haut niveau de l'entreprise
  - veiller à sa mise sur l'agenda du Conseil d'Administration / Comex de l'entreprise

Quelques bonnes pratiques…

Pour protéger son entreprise

- Instaurer **une gouvernance adaptée** au risque

- Mettre en place des **procédures et politiques** dédiées
  - plan de gestion de crise
  - plan de continuité d'activité

- **Connaître et comprendre le risque** en intégrant sa gestion dans le quotidien de l'entreprise
  - sensibiliser les équipes (à tous les niveaux de l'entreprise)
  - s'entraîner au travers de simulation de crises

- Garantir des **mesures de protection** efficaces
  - investir dans des outils de détection et de correction d'attaque performants
  - sécuriser l'architecture du si
  - protéger les données (intégrité, confidentialité, gestion des clés cryptographiques)

  + prendre en compte la menace physique et environnementale

Notification & Communication

Gestion de crise

Quelles notifications ?

CNIL

ANSSI

Violation de données à caractère personnel

Obligations liées à la violation de données à caractère personnel

1. Notification de la violation de données à l'autorité de contrôle (**72 heures**) (Article 33 du RGPD)

2. Communication de la violation de données aux personnes concernées (meilleurs délais) en cas de **risque élevé pour les personnes concernées** (Article 34 du RGPD)

3. Documentation de la violation de données **en toute hypothèse** (Article 33 du RGPD)

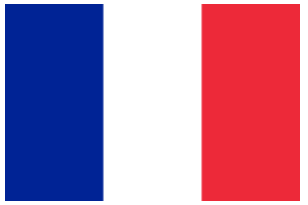
Cybersécurité

Les nouvelles réglementations européennes

Directives => doivent d'être **transposées** en droit national.

Règlements => sont d'application directe dans les Etats membres de l'Union européenne.

NB : Pour DORA, il y a un Règlement et une Directive.



Le **projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité** visant à transposer les Directives **NIS 2, DORA et REC** a été voté au Sénat le 12 mars 2025.

Le projet de loi a été adopté le 10 septembre 2025 par la Commission spéciale de l'Assemblée nationale (*en attente de l'examen en séance publique*)

Avec ce projet de loi, la France transpose trois directives :

- ✓ **NIS 2**
- ✓ **REC**
- ✓ **DORA** (Directive qui accompagne Règlement DORA, sur la résilience numérique opérationnel des entités du secteur financier)

Règlement DORA – Guide sur le cadre de surveillance des fournisseurs tiers critiques

Guide publié le 15 juillet 2025 par les autorités européennes de surveillance (AES) dans le cadre du règlement DORA.

Mise en place d'une gouvernance visant à garantir un suivi concerté, transparent et axé sur les risques des fournisseurs tiers critiques.

Etablissement d'un nouveau paradigme de surveillance directe des infrastructures TIC critiques, reposant sur un échange efficace entre les autorités européennes et nationales.


JC 2025 29

15 July 2025

Digital Operational Resilience Act (DORA):
Oversight of critical third-party providers

Guide on oversight activities

Consulter le guide

Volonté d'atténuer le risque systémique de concentration et d'harmoniser la gestion des risques liés aux tiers dans le domaine des TIC à l'échelle de l'Union européenne.

DORA - Règlement délégué (UE) 2025/532

Ce règlement a pour objet de préciser les éléments que les entités financières doivent évaluer lorsqu'elles sous-traitent des services relatifs aux technologies de l'information et de la communication (TIC) qui supportent des fonctions critiques ou importantes.

Que négocier ?

Une visibilité complète sur la chaîne de sous-traitance.

Des procédures d'approbation préalable pour les changements.

Des clauses de réversibilités renforcées.

La localisation des données dans l'UE si cela est possible.

Consulter le règlement

DORA - Règlement délégué (UE) 2025/532

Voir fiches pratiques

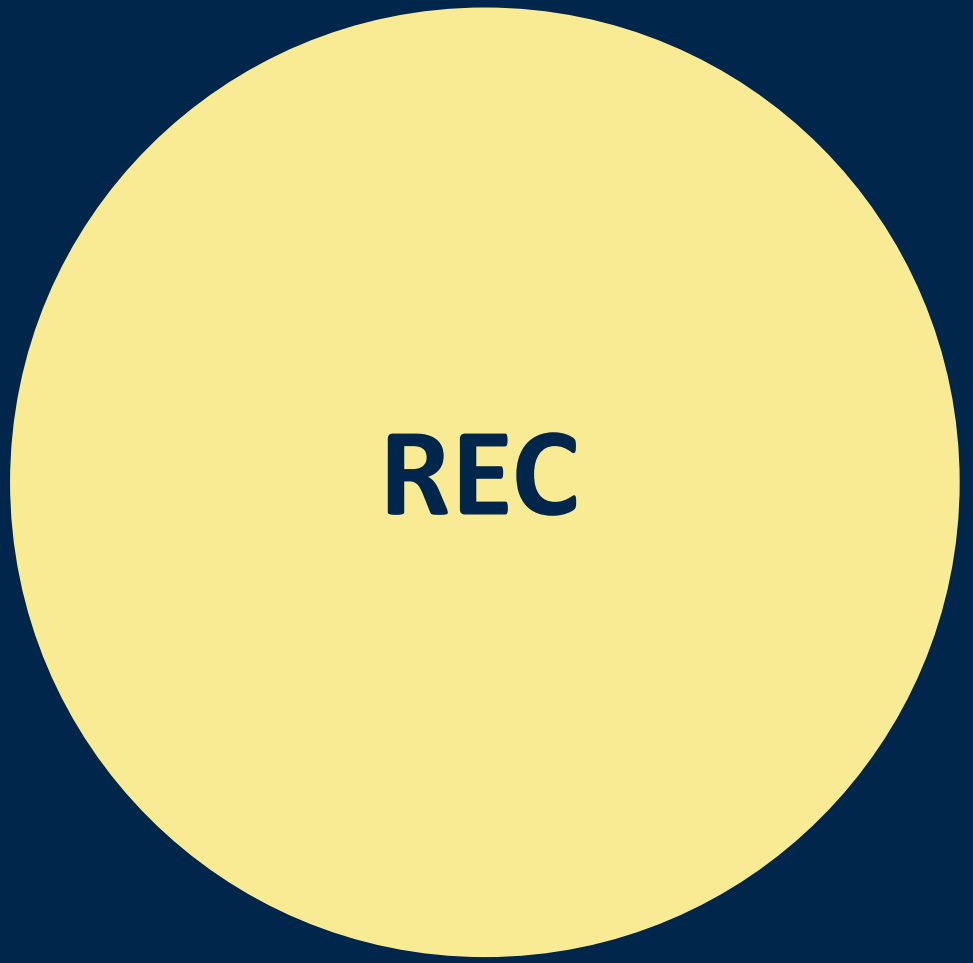
DORA et la chaîne de sous-traitance : Les précisions apportées par le Règlement délégué publié le 2 juillet 2025

Ce nouveau Règlement délégué vient préciser les modalités techniques de mise en œuvre des exigences relatives à la chaîne de sous-traitance, dans le cadre de la réglementation DORA.

Que faut-il retenir, d'une part, côté entités financières et, d'autre part, côté prestataires de services TIC ? Quelles bonnes pratiques contractuelles convient-il d'adopter

EN SAVOIR

Sécurité des infrastructures critiques



Directive dite « REC »

La Directive sur la résilience des entités critiques (REC), adoptée le 14 décembre 2022, est en cours de transposition en France *(projet de loi relatif à la résilience des infrastructures critique et au renforcement de la cybersécurité).*

Elle remplace la directive de 2008 portant sur le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection.

La Directive « REC » vise à

- réduire les **vulnérabilités** ;
- renforcer la **résilience physique des entités critiques.**

Point d'attention :

Les **entités critiques** sont définies par ladite directive et « fournissent des services indispensables pour maintenir les fonctions sociétales vitales, les activités économiques, la santé et la sécurité publiques ainsi que l'environnement ».

Directive dite « REC »

La directive sur la résilience des entités critiques a été adoptée le 14 décembre 2022, le même jour que le Règlement DORA.

La directive REC s'inscrit dans la **volonté européenne d'assurer un niveau plus élevé de sécurité et de renforcer l'harmonisation des mesures et la coopération entre États membres** – et avec les institutions européennes.

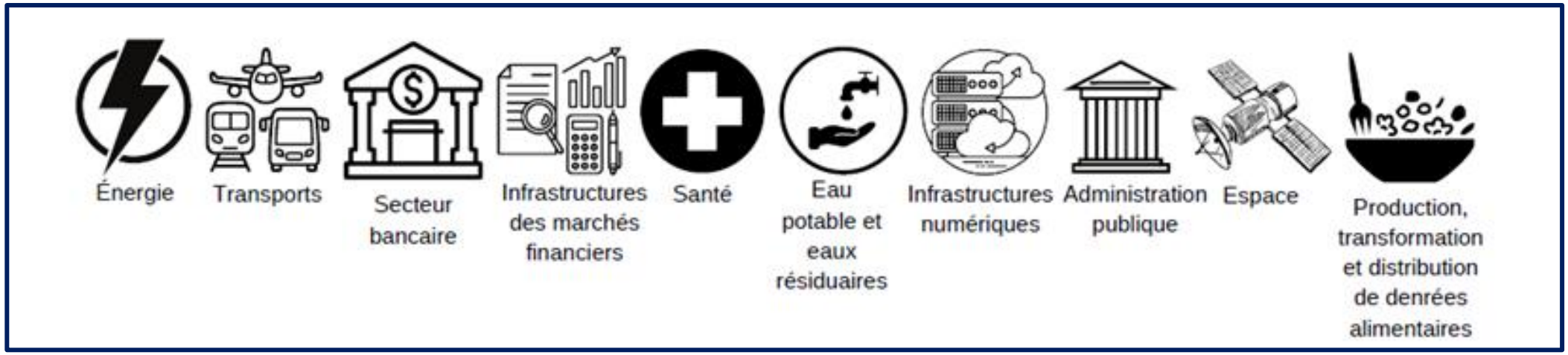
« La sécurité physique et la cybersécurité des entités critiques étant liées, les États membres veillent à ce que la présente directive [Directive REC] et la directive (UE) 2022/2555 [Directive NIS 2] soient mises en œuvre de manière coordonnée ». (article 1, 2. Directive REC)

Directive dite « REC » : quelles entités concernées ?

Les **entités critiques seront désignées par les États membres** dans les trois ans suivant l'adoption de la directive.

Ces dernières devront :

- ❖ fournir un ou plusieurs services essentiels,
- ❖ se trouver sur le territoire de l'État membre qui les désigne,
- ❖ il faudra également déterminer qu'un incident perturberait les services essentiels fournis par l'entité.



Création du statut d' **« entité critique d'importance européenne particulière » (article 17 de la directive) :** concernera les **entités fournissant des services essentiels dans au moins six États membres**. La Commission européenne établira la liste des entités critiques d'importance européenne particulière sur notification des États membres.

Directive dite « REC »

Obligations pour les entités critiques

En particulier :

- la notification à l'État membre concerné de tout incident perturbant les services essentiels fournis par l'entité en question ;
- l'organisation de contrôles et de tests afin d'éprouver les mécanismes de réponse aux attaques des entités ;
- l'évaluation des risques potentiels par les entités dans un délai de neuf mois après la notification par l'État membre concerné ;
- la prise de mesures en amont afin de « prévenir la survenance d'incidents » sous le contrôle de l'État membre concerné : protection physique des locaux, création de protocoles de gestion des risques, gestion adéquate du personnel…
- la vérification des antécédents des membres du personnel ;
- l'établissement de normes par les États membres encadrant l'usage de certaines technologies par les entités critiques.

Mise en conformité REC : quelles bonnes pratiques?

Gouvernance
Sensibilisation et Formation

Gestion adéquate du personnel

Gestion du risque en matière de sécurité physique des entités critiques
(protection physique des locaux, création de protocoles de gestion des risques…)

Planifier et chiffrer le budget alloué

Contrôles, tests, audits

Suivi des process et amélioration en continu

REC : Le calendrier

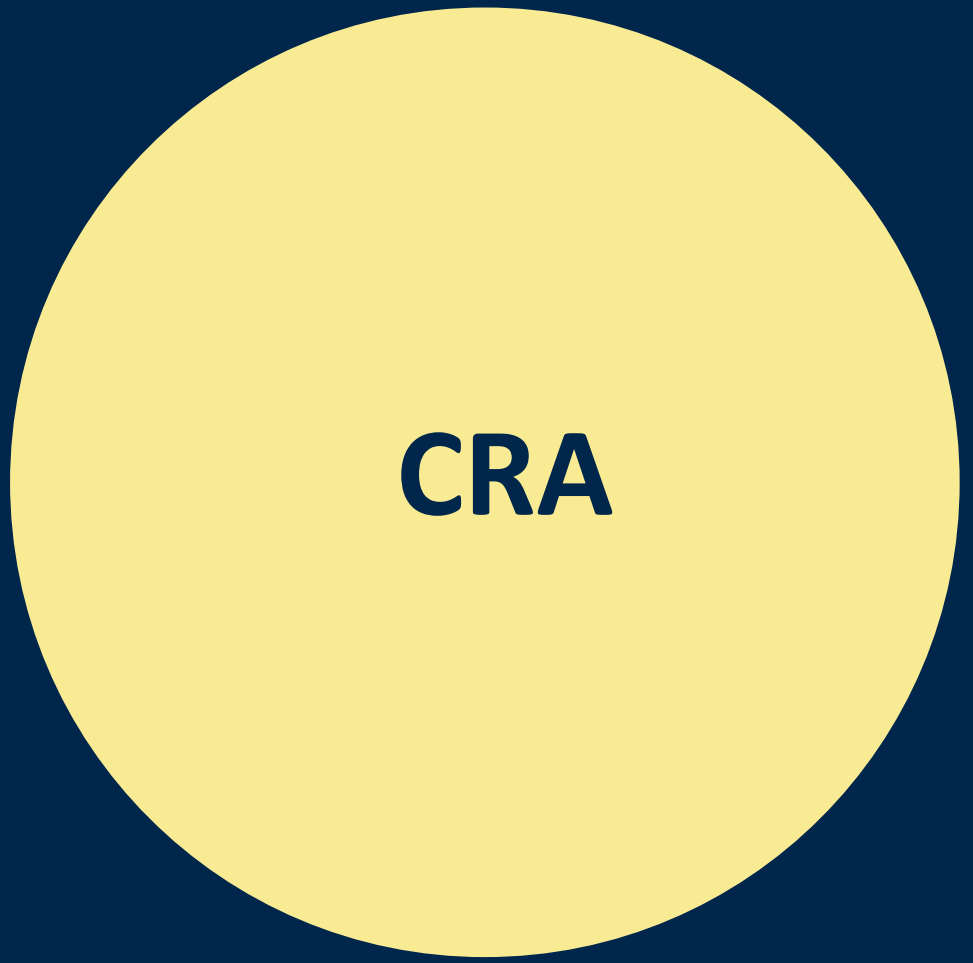
La Directive sur la résilience des entités critiques (REC), en cours de transposition en France, fera l'objet d'un rapport et d'un réexamen :

« Au plus tard le 17 juillet 2027, la Commission présentera au Parlement européen et au Conseil un rapport évaluant la mesure dans laquelle chaque État membre a pris les dispositions nécessaires pour se conformer à la présente directive » (article 25, Directive REC).

Dans le cadre de ce réexamen, la Commission se concentrera sur :

- la valeur ajoutée de ce texte,
- son impact en vue de garantir la résilience des entités critiques,
- et déterminera si l'annexe de la directive relative au champ d'application devrait être modifiée.

Cybersécurité



Cyber Resilience Act : pour la sécurité des produits connectés

Le **Règlement sur la Cyber résilience adopté le 23 octobre 2024** (et publié le 20 novembre 2024) vise à compléter NIS 2 et DORA en **protégeant les consommateurs et les entreprises** qui utilisent des **produits** ou des **logiciels** comportant un **composant numérique**.

Le CRA concerne **tous les produits connectés (directement ou indirectement)** et comprend des exceptions : SaaS, secteur médical, aviation.

Il entrera en application à partir du **11 décembre 2027.** A l'exception des *Obligations en matière de communication d'informations incombant aux fabricants* (article 14) qui seront applicables à partir du **11 septembre 2026** ; et des dispositions relatives à la *notification des organismes d'évaluation de la conformité* (Chapitre IV, article 34 à 51) qui s'appliqueront à partir du **11**

3 piliers du texte :

1. **Cybersecurity by design** (produits conçus, développés et fabriqués pour atteindre un certain niveau de cybersécurité)
2. **information de l'utilisateur** pour garantir une utilisation sécurisée
3. **Politiques de gestion des vulnérabilités** (cartographie des risques, réalisation de test réguliers, etc.)

Responsabilité pour :

- Le fabriquant
- L'importateur
- Le distributeur

Cyber Resilience Act : calendrier de mise en oeuvre

Le Cyber resilience Act est adopté

23/11/2024

Entrée en application

11/06/2026

Dispositions relatives à la notification des organismes d'évaluation de la conformité (Chapitre IV, article 34 à 51)

11/09/2026

Obligations en matière de communication d'informations / signalements incombant aux fabricants (article 14)

11/12/2027

Entrée en application des autres dispositions du CRA

3 ans après entrée en vigueur du CRA (puis tous les 4 ans)

La Commission fournira au Parlement un rapport d'audit concernant la bonne mise en œuvre et application du CRA

Cyber Resilience Act : les sanctions encourues

Violation des critères de conformité ou des obligations du fabricant	Jusqu'à **15 millions** d'euros ou **2,5% du CA** annuel total
Violation de toute autre obligation du règlement	Jusqu'à **10 millions** d'euros ou **2% du CA** annuel total
Fournitures d'informations incomplètes, incorrectes ou trompeuses à l'organisme d'évaluation du produit ou à l'autorité de surveillance du marché	Jusqu'à **5 millions** d'euros ou **1% du CA** annuel total
Produit non conforme ou présentant un risque aux yeux de l'autorité de surveillance du marché	Restriction, suspension ou interdiction de la **disponibilité du produit** sur le marché

Intelligence artificielle

Focus sur le Règlement européen sur l'intelligence artificielle

IA : quels risques ?

Les usages de l'IA **ne sont pas sans risques** et soulèvent des **questions juridiques**, notamment au regard des **droits fondamentaux** (non-discrimination, respect de la vie privée…), de la protection des données à caractère personnel, des droits de propriété intellectuelle, etc.

Risques pour les **libertés fondamentales** :

- protection des **données personnelles** compromise par l'exploitation massive de données
- **potentielles atteintes à la vie privée** notamment par l'identification d'individu dans l'espace public grâce à la vidéosurveillance « augmentée »

Risques de **reproduction de biais discriminatoires** et de la **stigmatisation** de certaines populations :

- par le **choix de données** avec lesquelles sont alimentés les systèmes d'IA
- par le **paramétrage** subjectif des algorithmes

Risques propres à **l'environnement numérique :**

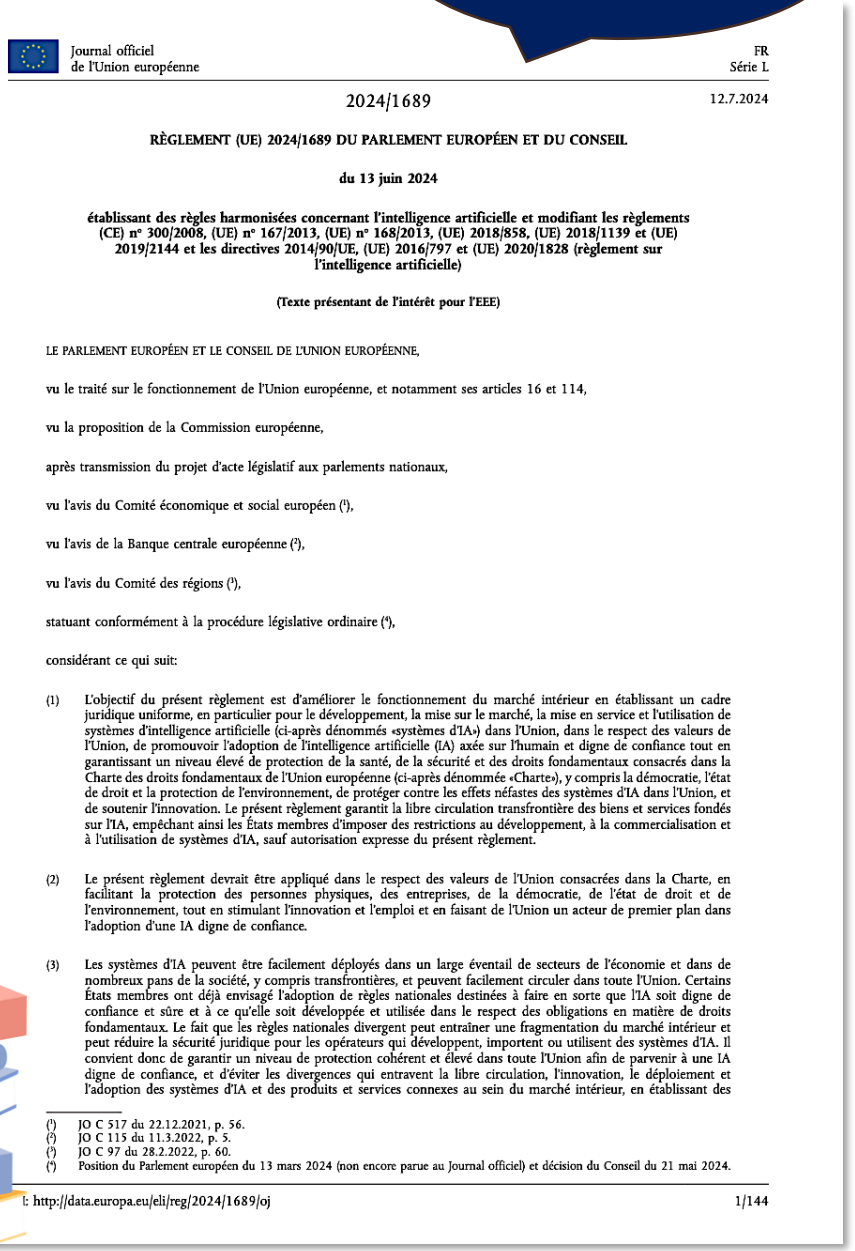
- **vulnérabilité** des services publics accru par leur numérisation (cyberattaque)
- **coût énergétique** de l'exploitation des outils d'IA

Le Règlement européen sur l'IA

Consulter le règlement

Il vise à « **améliorer le fonctionnement du marché intérieur et de promouvoir l'adoption d'une intelligence artificielle (IA) axée sur l'humain et digne de confiance**, tout en garantissant un **niveau élevé de protection de la santé, de la sécurité et des droits fondamentaux** consacrés dans la Charte européenne des droits fondamentaux, notamment la démocratie, l'état de droit et la protection de l'environnement, contre les effets néfastes des systèmes d'IA dans l'Union, et en soutenant l'innovation ». (art. 1, RIA)

À savoir : Le RIA est le premier règlement consacré à l'IA, publié le 12 juillet 2024 au Journal officiel de l'Union européenne.



Journal officiel de l'Union européenne — FR Série L

2024/1689 — 12.7.2024

RÈGLEMENT (UE) 2024/1689 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 13 juin 2024

établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle)

(Texte présentant de l'intérêt pour l'EEE)

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment ses articles 16 et 114,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen (1),

vu l'avis de la Banque centrale européenne (2),

vu l'avis du Comité des régions (3),

statuant conformément à la procédure législative ordinaire (4),

considérant ce qui suit:

(1) L'objectif du présent règlement est d'améliorer le fonctionnement du marché intérieur en établissant un cadre juridique uniforme, en particulier pour le développement, la mise sur le marché, la mise en service et l'utilisation de systèmes d'intelligence artificielle (ci-après dénommés «systèmes d'IA») dans l'Union, dans le respect des valeurs de l'Union, de promouvoir l'adoption de l'intelligence artificielle (IA) axée sur l'humain et digne de confiance tout en garantissant un niveau élevé de protection de la santé, de la sécurité et des droits fondamentaux consacrés dans la Charte des droits fondamentaux de l'Union européenne (ci-après dénommée «Charte»), y compris la démocratie, l'état de droit et la protection de l'environnement, de protéger contre les effets néfastes des systèmes d'IA dans l'Union, et de soutenir l'innovation. Le présent règlement garantit la libre circulation transfrontière des biens et services fondés sur l'IA, empêchant ainsi les États membres d'imposer des restrictions au développement, à la commercialisation et à l'utilisation de systèmes d'IA, sauf autorisation expresse du présent règlement.

(2) Le présent règlement devrait être appliqué dans le respect des valeurs de l'Union consacrées dans la Charte, en facilitant la protection des personnes physiques, des entreprises, de la démocratie, de l'état de droit et de l'environnement, tout en stimulant l'innovation et l'emploi et en faisant de l'Union un acteur de premier plan dans l'adoption d'une IA digne de confiance.

(3) Les systèmes d'IA peuvent être facilement déployés dans un large éventail de secteurs de l'économie et dans de nombreux pans de la société, y compris transfrontières, et peuvent facilement circuler dans toute l'Union. Certains États membres ont déjà envisagé l'adoption de règles nationales destinées à faire en sorte que l'IA soit digne de confiance et sûre et à ce qu'elle soit développée et utilisée dans le respect des obligations en matière de droits fondamentaux. Le fait que les règles nationales divergent peut entraîner une fragmentation du marché intérieur et peut réduire la sécurité juridique pour les opérateurs qui développent, importent ou utilisent des systèmes d'IA. Il convient donc de garantir un niveau de protection cohérent et élevé dans toute l'Union afin de parvenir à une IA digne de confiance, et d'éviter les divergences qui entravent la libre circulation, l'innovation, le déploiement et l'adoption des systèmes d'IA et des produits et services connexes au sein du marché intérieur, en établissant des

(1) JO C 517 du 22.12.2021, p. 56.
(2) JO C 115 du 11.3.2022, p. 5.
(3) JO C 97 du 28.2.2022, p. 60.
(4) Position du Parlement européen du 13 mars 2024 (non encore parue au Journal officiel) et décision du Conseil du 21 mai 2024.

ELI: http://data.europa.eu/eli/reg/2024/1689/oj — 1/144

Règlement européen sur l'IA : Champ d'application

Tous secteurs d'activités, tous les acteurs de la chaîne

Le législateur européen a choisi que ce champ soit **le plus large possible**, afin d'atteindre les objectifs du Règlement.

Tous secteurs d'activités

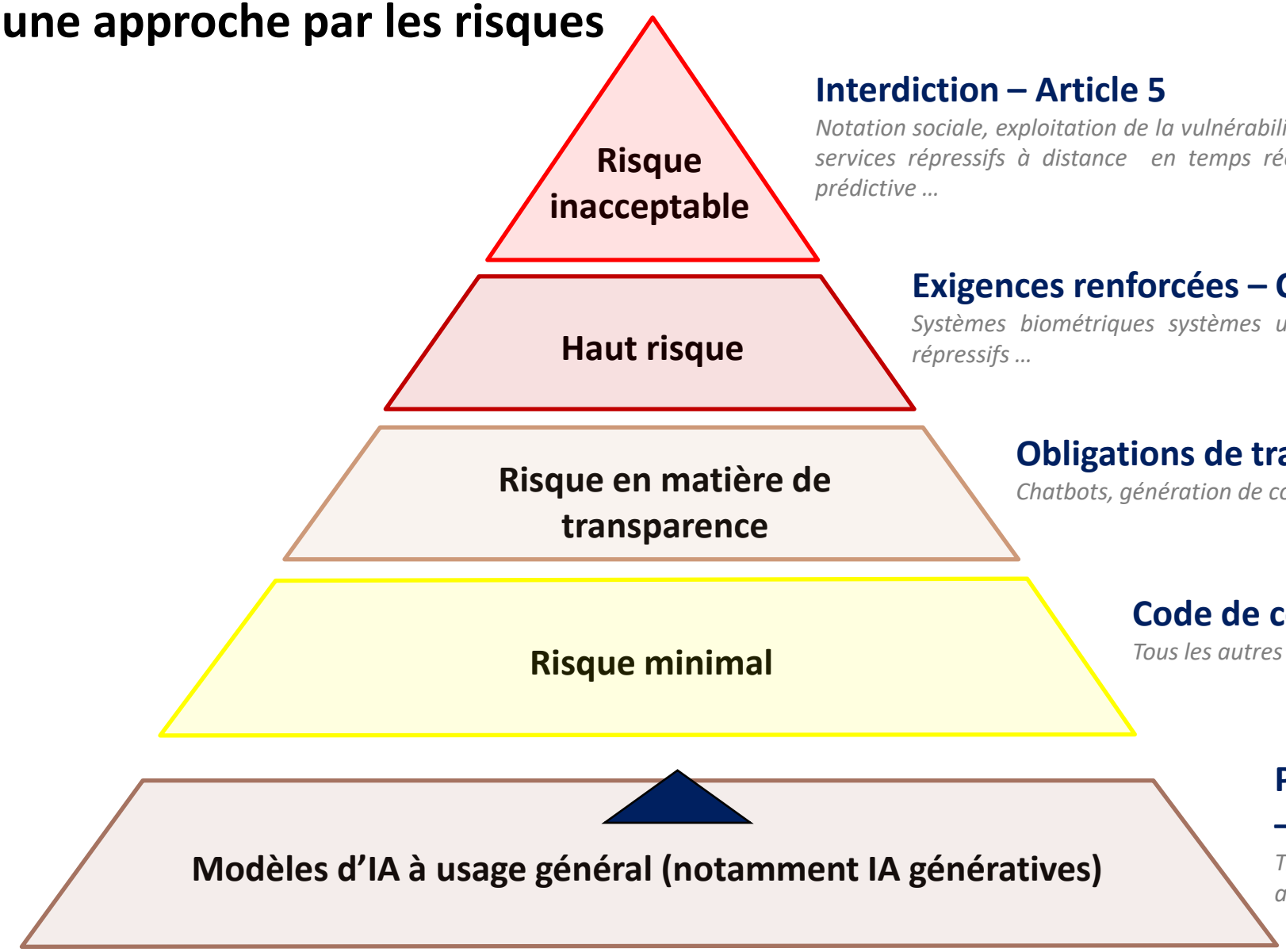
- A l'exception de certaines utilisations d'IA, ex : « exclusivement à des fins militaires, de défense ou de sécurité nationale » (cf. **article 2, Champ d'application**)

Toute la chaîne d'approvisionnement, tous les acteurs

- Regroupés sous le terme d' « **opérateurs** » : fournisseur, fabricant de produits, déployeur, mandataire, importateur ou distributeur (**article 3, Définitions**)

- Un **système d'IA** est défini comme « *un système automatisé qui est conçu pour fonctionner à différents niveaux d'autonomie et peut faire preuve d'une capacité d'adaptation après son déploiement, et qui, pour des objectifs explicites ou implicites, déduit, à partir des entrées qu'il reçoit, la manière de générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels* » (**article 3, Définitions**).

RIA, une approche par les risques



Interdiction – Article 5

Notation sociale, exploitation de la vulnérabilité des personnes, identification biométrique par les services répressifs à distance en temps réel dans des espaces accessibles au public, police prédictive …

Exigences renforcées – Chapitre III (article 6 et suivants)

Systèmes biométriques systèmes utilisés dans le recrutement ou pour des usages répressifs …

Obligations de transparence – Article 50

Chatbots, génération de contenu artificiel …

Code de conduite – Article 95

Tous les autres systèmes d'A

Plusieurs niveaux d'obligations – Chapitre V (articles 51 à 56)

Transparence, documentation, évaluation et atténuation des risques systémiques …

Commission européenne, *législation sur l'IA,* https://digital-strategy.ec.europa.eu/fr/policies/regulatory-framework-ai
Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle)

Le règlement européen sur l'IA : les acteurs

➔ *Les définitions des « opérateurs »*

FOURNISSEUR

- « une personne physique ou morale, une autorité publique, une agence ou tout autre organisme qui développe ou fait développer un système d'IA ou un modèle d'IA à usage général et le met sur le marché ou met le système d'IA en service sous son propre nom ou sa propre marque, à titre onéreux ou gratuit; »

DEPLOYEUR

- « une personne physique ou morale, une autorité publique, une agence ou un autre organisme utilisant sous sa propre autorité un système d'IA sauf lorsque ce système est utilisé dans le cadre d'une activité personnelle à caractère non professionnel; »

MANDATAIRE

- « une personne physique ou morale située ou établie dans l'Union ayant reçu et accepté un mandat écrit d'un fournisseur de système d'IA ou de modèle d'IA à usage général pour s'acquitter en son nom des obligations et des procédures établies par le présent règlement; »

IMPORTATEUR

- « une personne physique ou morale située ou établie dans l'Union qui met sur le marché un système d'IA qui porte le nom ou la marque d'une personne physique ou morale établie dans un pays tiers; ».

DISTRIBUTEUR

- « une personne physique ou morale faisant partie de la chaîne d'approvisionnement , autre que le fournisseur ou l'importateur, qui met un système d'IA à disposition sur le marché de l'Union; »

+ FABRICANTS DE PRODUITS qui mettent sur le marché ou mettent en service un système d'IA en même temps que leur produit et sous leur propre nom ou leur propre marque.

Art. 2 & 3, RIA

Calendrier d’application de l’IA ACT

1er août 2024 : Entrée en vigueur du règlement.

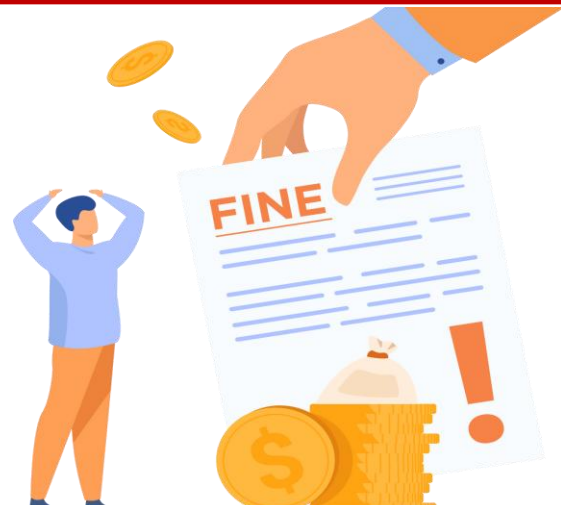
2 février 2025 : Interdiction des systèmes d’IA présentant des risques jugés inacceptables.

2 août 2025 : Mise en place des règles pour les modèles d’IA à usage général et désignation des autorités compétentes dans chaque État membre.

2 août 2026 : Application complète aux systèmes d'IA à haut risque déjà identifiés, tels que ceux utilisés dans la biométrie, les infrastructures critiques, l'éducation, l'emploi ou la justice. Cette date marque également la mise en place de *bacs à sable réglementaires* pour accompagner les entreprises.

2 août 2027 : Application aux systèmes d'IA à haut risque incorporés dans certains produits réglementés, comme les jouets, les dispositifs médicaux, les machines.

Focus sur les sanctions



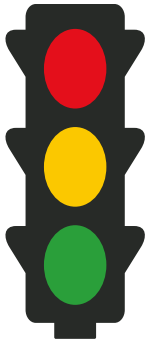
RIA : Quelles sanctions ?

En cas de non-respect des obligations prévues par le RIA, des sanctions sont prévues par son article 99 (et ce, indépendamment d'un risque d'image et réputationnel)

Concernant les **pratiques interdites en matière d'IA (article 5) :** Les amendes administratives peuvent atteindre jusqu'à **35 millions d'euros** ou, si l'auteur de l'infraction est une entreprise, jusqu'à **7 % de son chiffre d'affaires annuel mondial total** réalisé au cours de l'exercice précédent, le montant le plus élevé étant retenu.

La **non-conformité aux dispositions** du Règlement, **autres que celles énoncées à l'article 5,** peut donner lieu à une **amende administrative pouvant aller jusqu'à 15 000 000 EUR ou, si l'auteur de l'infraction est une entreprise, jusqu'à 3 % de son chiffre d'affaires annuel mondial** total réalisé au cours de l'exercice précédent, le montant le plus élevé étant retenu.

La **fourniture d'informations inexactes, incomplètes ou trompeuses aux organismes notifiés ou aux autorités nationales compétentes en réponse à une demande** fait l'objet d'une amende administrative pouvant aller jusqu'à **7 500 000 EUR** ou, si l'auteur de l'infraction est une entreprise, jusqu'à **1 % de son chiffre d'affaires** annuel mondial total réalisé au cours de l'exercice précédent, le montant le plus élevé étant retenu. *Dans le cas des PME et start-up, pour les sanctions prévues à l'article 99, c'est le montant le plus faible qui sera retenu.*



Intelligence artificielle : assurer sa conformité juridique

Au-delà du règlement européen sur l'IA…

- Propriété intellectuelle
- Droit des données personnelles
- Droit du travail
- Droit de la cybersécurité
- RSE

Vols de données par des collaborateurs internes à la société :

Les recommandations de la DGSI

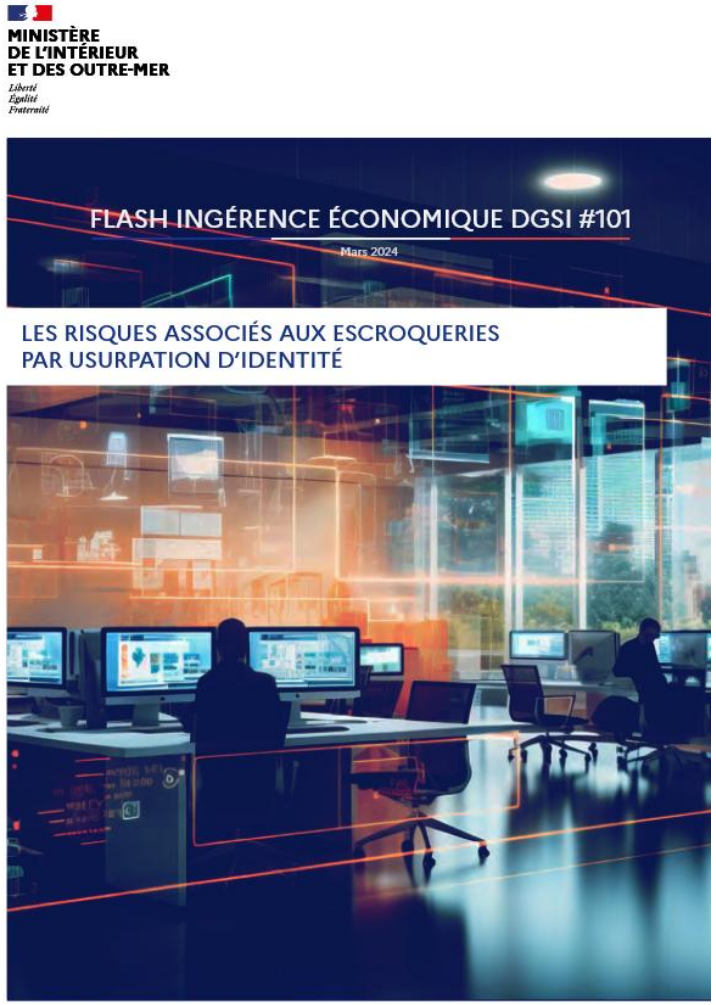
- ✓ Le risque de vol par un collaborateur interne (employé, stagiaire, prestataire, etc.) est réel. Les auteurs de vols peuvent recourir à des captations pour de multiples raisons (revente, réutilisation pour le compte d'un nouvel employeur ou pour la création d'une entreprise concurrente, vengeance, etc.).

- ✓ Or, la perte de données sensibles peut avoir d'importantes conséquences pour l'activité des entreprises victimes : perte de savoir-faire stratégique, préjudices financier ou commercial, atteinte à la réputation, perte de confiance des clients, coût des poursuites juridiques, etc..

- ✓ Ce Guide, publié par la DGSI en octobre 2024, vise à sensibiliser et informer les entités sur ces risques, Il inclut des préconisations, visant à :
  - Renforcer la protection de ses données sensibles pour prévenir les risques de vols ;
  - Déposer plainte si un vol de données est

Les risques associés aux escroqueries par usurpation d'identité

Les recommandations de la DGSI 2024



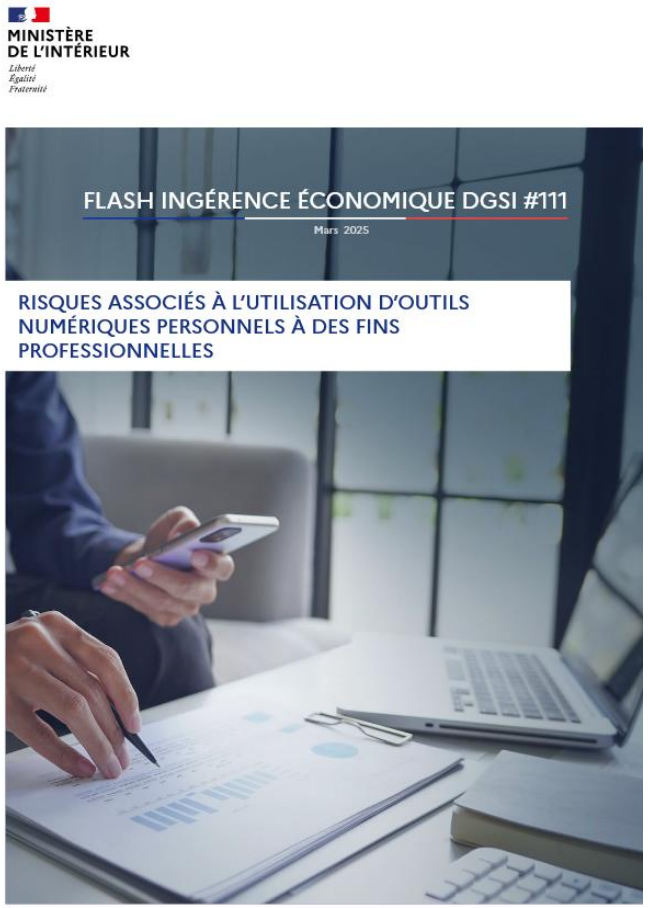
- ✓ Le risque d'escroquerie par usurpation d'identité est bien réel. Les auteurs de ces escroqueries peuvent recourir à des techniques d'ingénierie sociale particulièrement sophistiquées (faux emails, appels ou visio-conférences falsifiées, deepfakes, etc.) pour obtenir des transferts de fonds ou des informations sensibles. Ces attaques peuvent viser tout type d'organisation : start-up, PME, grands groupes, laboratoires, etc. Les motivations de ces escroqueries sont diverses : détournement d'argent, captation d'informations confidentielles, affaiblissement d'un concurrent, ou atteinte à la réputation

- ✓ Or, les conséquences pour les entreprises ciblées peuvent être graves : pertes financières directes, atteinte à la réputation, exploitation d'informations sensibles, remise en cause de la confiance des clients ou partenaires, etc.

- ✓ Ce Guide, publié par la DGSI en mars 2024, vise à sensibiliser et informer les entreprises et organismes sur ces risques croissants. Il inclut des préconisations concrètes visant à :
  - Prévenir les tentatives d'escroquerie (procédure, test, sensibilisation, usage…);
  - Alerter et déposer plainte en cas de suspicion d'escroquerie;

Risques associés à l'utilisation d'outils numériques personnels à des fins professionnelles

Les recommandations de la DGSI 2025



- ✓ Le recours aux outils numériques personnels à des fins professionnelles expose les entreprises à des risques importants. Ces pratiques, souvent non encadrées, rendent les données sensibles vulnérables en raison d'une protection insuffisante des appareils personnels (absence de chiffrement, d'authentification forte, etc.). Les incidents peuvent résulter de négligences (utilisation d'un ordinateur familial sans sécurité), de vols (ordinateur personnel contenant des données sensibles), ou encore d'ingérences étrangères (saisie d'un téléphone en douane).

- ✓ Ces situations peuvent avoir des conséquences graves pour les entreprises concernées : accès non autorisé aux bases de données, exfiltration d'informations confidentielles, perte de compétitivité, atteinte à la réputation, rupture de relations avec des prestataires, etc.

- ✓ Ce Guide, publié par la DGSI en mars 2025, vise à sensibiliser les entreprises aux dangers du « Bring Your Own Device » (BYOD) et recommande notamment de :

- Sensibiliser les salariés aux bonnes pratiques d'hygiène numérique et à la séparation des usages personnels et professionnels ;
- Adapter les politiques internes de sécurité pour encadrer le recours aux appareils personnels dès l'embauche ;
- Prévoir des mesures en cas de vol, de compromission ou de saisie d'un appareil personnel ;
- Mettre en place des dispositifs de cloisonnement, de gestion à distance, et de

Le facteur humain, principal vecteur de la compromission des systèmes d'information

Les recommandations de la DGSI 2025

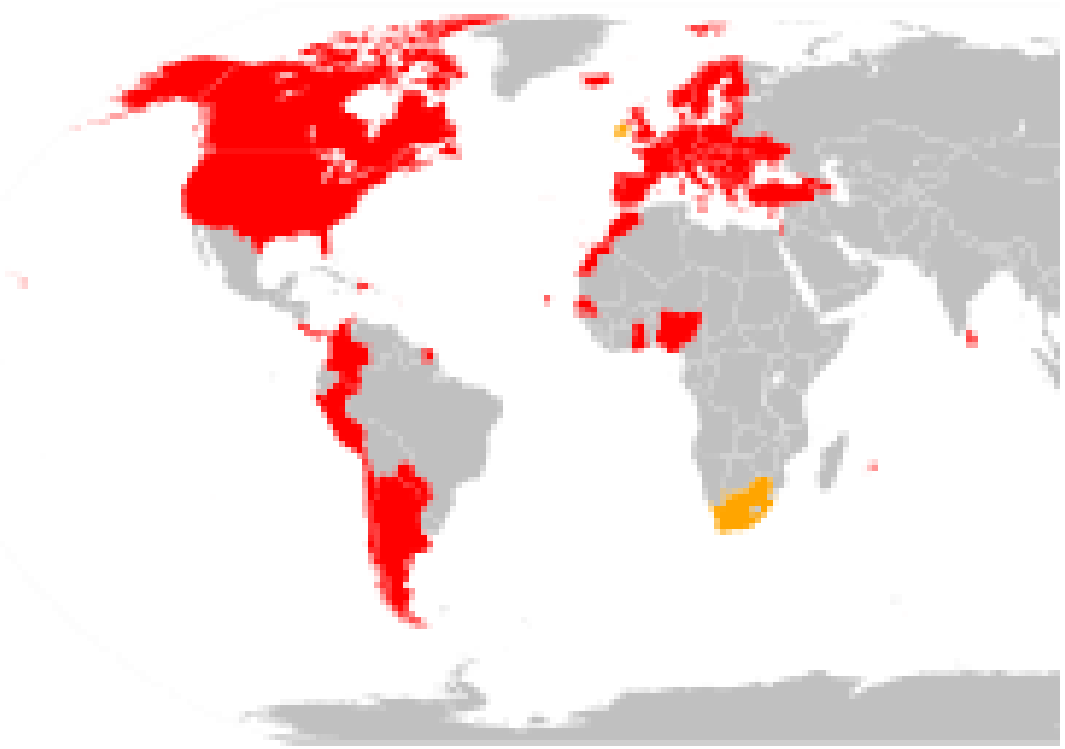
✓ Le facteur humain constitue la principale faille dans la sécurité des systèmes d'information. Qu'elles soient dues à la négligence, à l'ignorance ou à une volonté délibérée de transgresser les règles, ces erreurs humaines facilitent les attaques informatiques. De nombreuses compromissions pourraient être évitées si les consignes de sécurité étaient correctement appliquées.

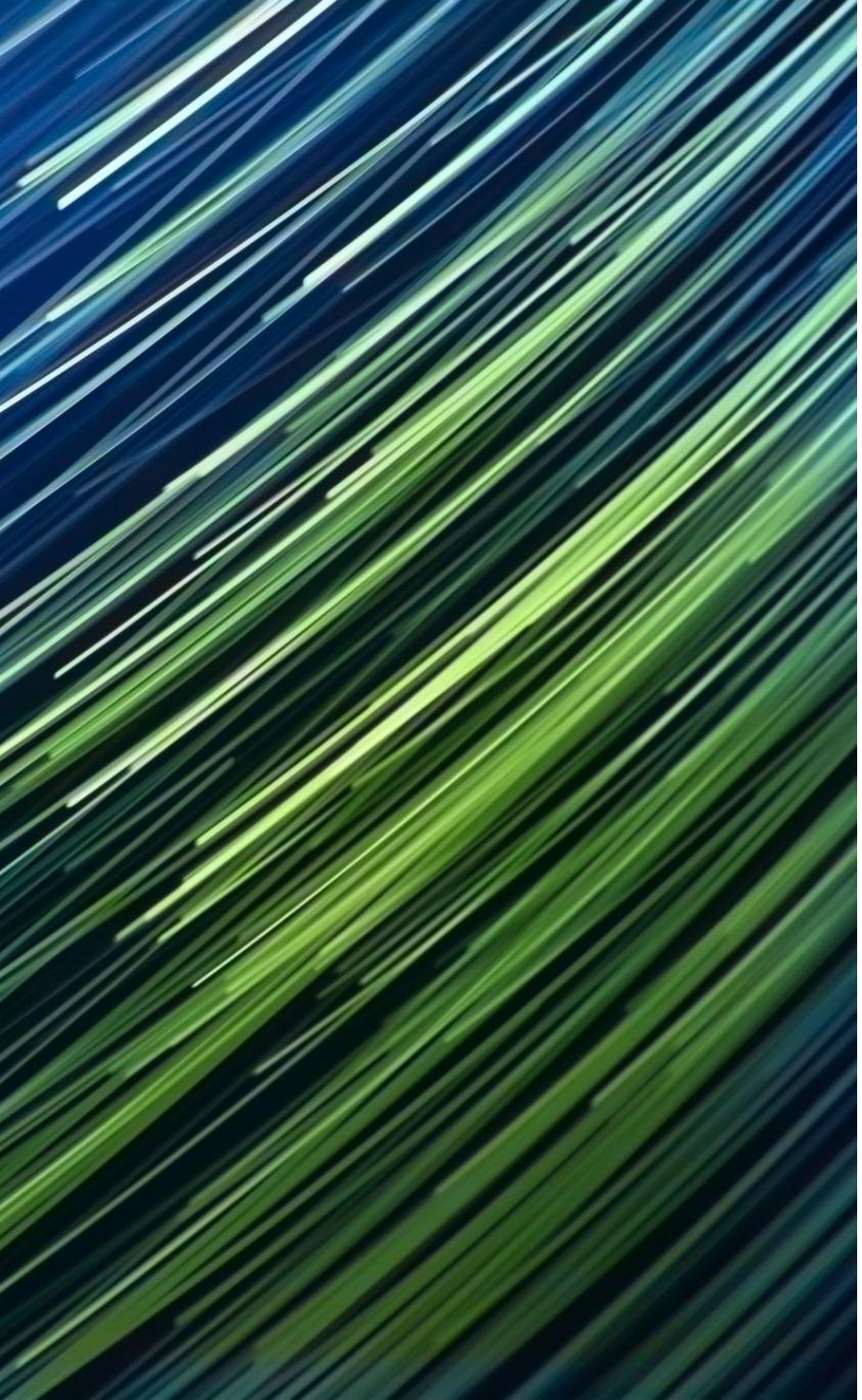
✓ Ces incidents peuvent avoir des conséquences graves : fuites de données sensibles, perte de propriété intellectuelle, atteinte à la réputation ou encore compromission de systèmes critiques.

✓ Ce Guide, publié par la DGSI en avril 2025, vise à alerter les entités sur ces risques. Il inclut des préconisations pour :

- Renforcer la culture de sécurité informatique des collaborateurs (sensibilisation, formation, charte informatique, etc.) ;
- Cloisonner les accès et restreindre les privilèges au strict nécessaire ;
- Adopter des mesures techniques robustes (audit de sécurité, COS, contrôle des périphériques USB, hébergement sécurisé

Convention de Budapest sur la cybercriminalité





Exemples d’affaires cyber

Les paiements en cryptos deviennent « standards » dans le monde criminel du fait de leur efficacité

Les cryptoactifs offrent aux auteurs d’activités illicites, une combinaison unique d’anonymat, de rapidité et de sécurité, qui leur permet de contourner les systèmes financiers traditionnels et les contraintes juridiques. »

Les plateformes d’échange de crypto-monnaies (ou "*crypto-exchanges*") offrent un levier pour les délinquants et notamment narcotrafiquants. Alors que certaines sont désormais soumises à des régulations strictes, d’autres, dites non régulées, permettent de procéder à des transactions en toute discrétion, ce qui les rend particulièrement attractives pour les criminels. La présence d’échanges décentralisés (DEX), où aucune entité centrale ne contrôle les transactions, renforce cette possibilité de contourner les autorités.


This Website Has Been Seized
Cyber : Europol met fin à la marketplace Manson Market !
POLITIE

Merci de votre attention
Des questions?