WISG

Workshop interdisciplinaire sur la sécurité globale

25 & 26 mars 2026 • EuraTechnologies Lille

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

anr agence nationale de la recherche
AU SERVICE DE LA SCIENCE

FRANCE 2030

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR, DE LA RECHERCHE ET DE L'ESPACE

PREMIER MINISTRE
Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Cybercriminalité Actualités et réponses juridiques

Myriam Quéméner , magistrat judiciaire honoraire , docteur en droit

Un fléau en expansion, multiplication des cyberattaques

Une délinquance boostée par l'IA

Industrialisation et automatisation du phénomène

Après FICOBA, une nouvelle cyberattaque secoue l'État français. En piratant un service de l'État, un cybercriminel est parvenu à voler des informations relatives à la CAF (Caisse d'Allocations Familiales). Les données des bénéficiaires au RSA ont été compromises, dont le numéro de sécurité sociale, le matricule allocataire, et les coordonnées complètes.

Plan

- Les infractions d'ASTAD, classiques et nouvelles
- Cybercriminalité : définitions et enjeux actuels
- Les procédures adaptées au numérique
- La recherche de la preuve numérique
- La dimension internationale de la lutte contre la cybercriminalité

Circonstances aggravantes

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)

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

226-18 du CP
Collecte 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

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

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

Diffusion de contenus illicites:
Diffamation de presse (honneur et considération) et atteinte à l'e-réputation
- Usage de toute données 226-4-1
- Incitation à la haine raciale
- Pédopornographie

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 désormais 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* ». De plus, 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.

Deux techniques spéciales d'investigation sont

- La loi n° 2025-532, 13 juin 2025 , visant à sortir la France du piège du narcotrafic, art. 38 et 39) instaure une nouvelle technique spéciale d'enquête consistant à activer à distance un appareil électronique afin de capter l'image ou les paroles des personnes surveillées**.** Cette procédure est possible : en matière de trafic de stupéfiants ; d'actes de terrorisme ; d'atteintes aux intérêts fondamentaux de la Nation ; meurtres ou tortures commis en bande organisée ; enlèvements et séquestrations ; armes et d'explosifs ; blanchiment de ces infractions et association de malfaiteurs ayant pour but de les préparer).
- **Le Conseil constitutionnel** a **émis une réserve d'interprétation en subordonnant le recours à la technique à une condition de gravité supplémentaire à savoir que les délits visés par la liste soient commis en bande organisée et punis d'au moins 5 ans d'emprisonnement (Cons. const., 12 juin 2025, n° 2025-885 DC, § 319),**
- CPP, art. 706-73, 1° à 6° et 11° à 12

NIS 2 : pour un niveau de cybersécurité élevé

Adoptée et publiée au Journal Officiel de l'Union européenne en décembre 2022, la **Directive 2022/2555 dite « NIS 2 »** *(Network & Information Security)* abroge la directive NIS 1 du 6 juillet 2016 qui avait défini un **régime européen de la cybersécurité.**

NIS 2 : EE & EI

Entités essentielles	Entités importantes
• Espace • Santé • Banques et infrastructures de marchés financiers • Transports • Eau potable/usée • Infrastructures numériques • Énergie • Administration publique	• Fabricants, producteurs, distributeurs de produits chimiques • Service postal • Services numériques • Gestion des déchets • Fabricants de produits spécifiques (équipement de transport, informatique, dispositif médical)

Objectifs-clés :

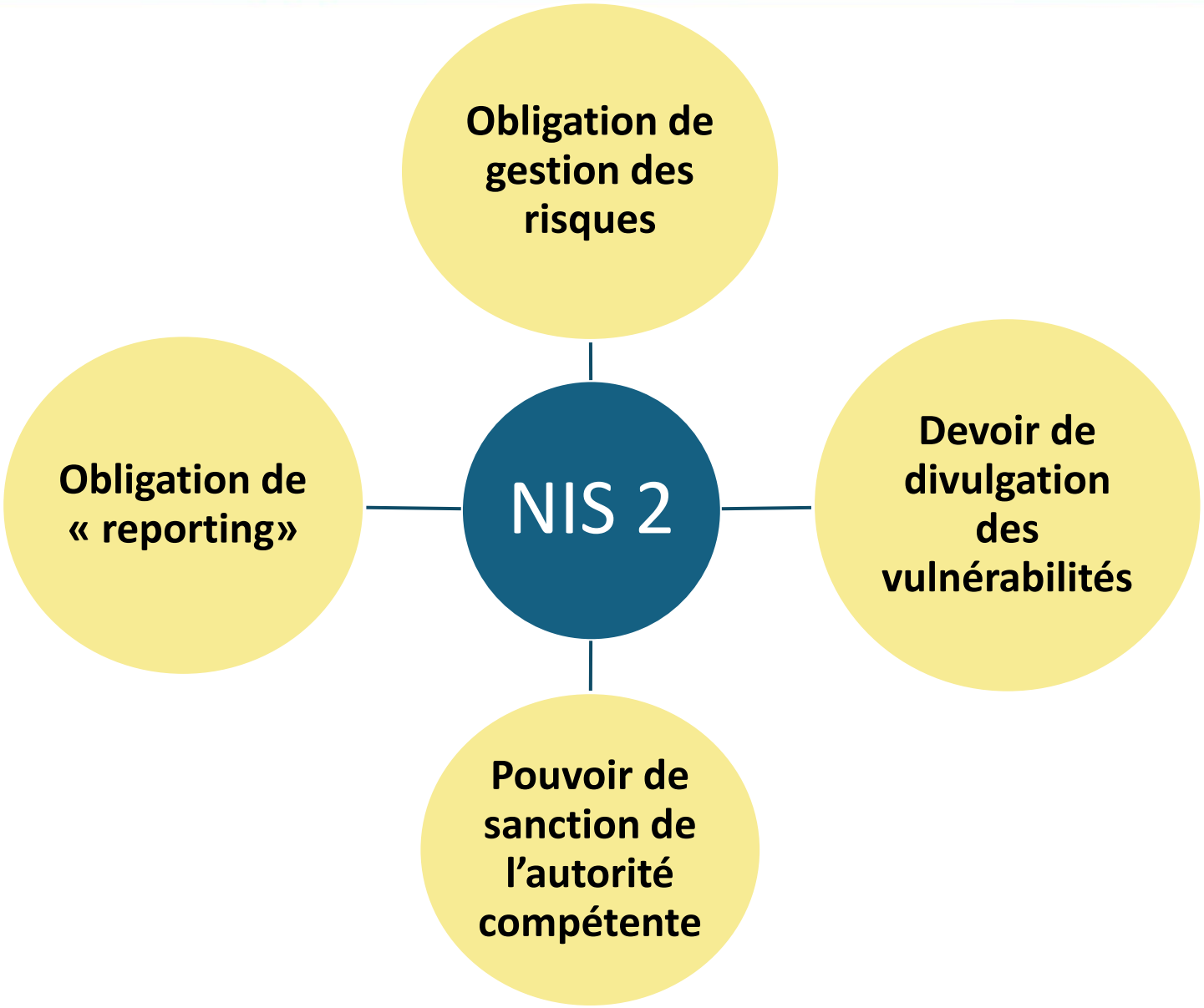
1. Moderniser le cadre juridique existant pour l'adapter à la digitalisation croissante et à l'évolution des menaces en matière de cybersécurité ;

2. Etendre le champ d'application de la directive NIS 1 à de nouveaux secteurs et entités ;

3. Améliorer la résilience et les capacités de réaction aux incidents des entités publiques et privées ;

4. ainsi que des autorités compétentes et de l'UE dans son ensemble ➔ Favoriser le partage de l'information et des connaissances, afin de renforcer la capacité collective de préparation et de réponse aux attaques.

Les principes-clés de NIS 2

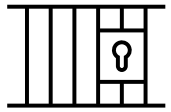


Point d'attention : la *supply chain*

Prise en compte des **risques associés à la chaîne de valeur (sous-traitants, fournisseurs, etc.)**
→ NIS 2 prévoit des obligations de gestion des risques associés à l'ensemble des organismes tiers appartenant à la chaîne d'approvisionnement *(« supply chain »)* des acteurs concernés par la directive.

NIS 2 : Pouvoir de sanction de l'autorité compétente à l'échelle nationale*

Entité Importante	Entité Essentielle
• 7 millions € ou • 1.4% du CA mondial total	• 10 millions € ou • 2% du CA mondial total



La responsabilité des dirigeants

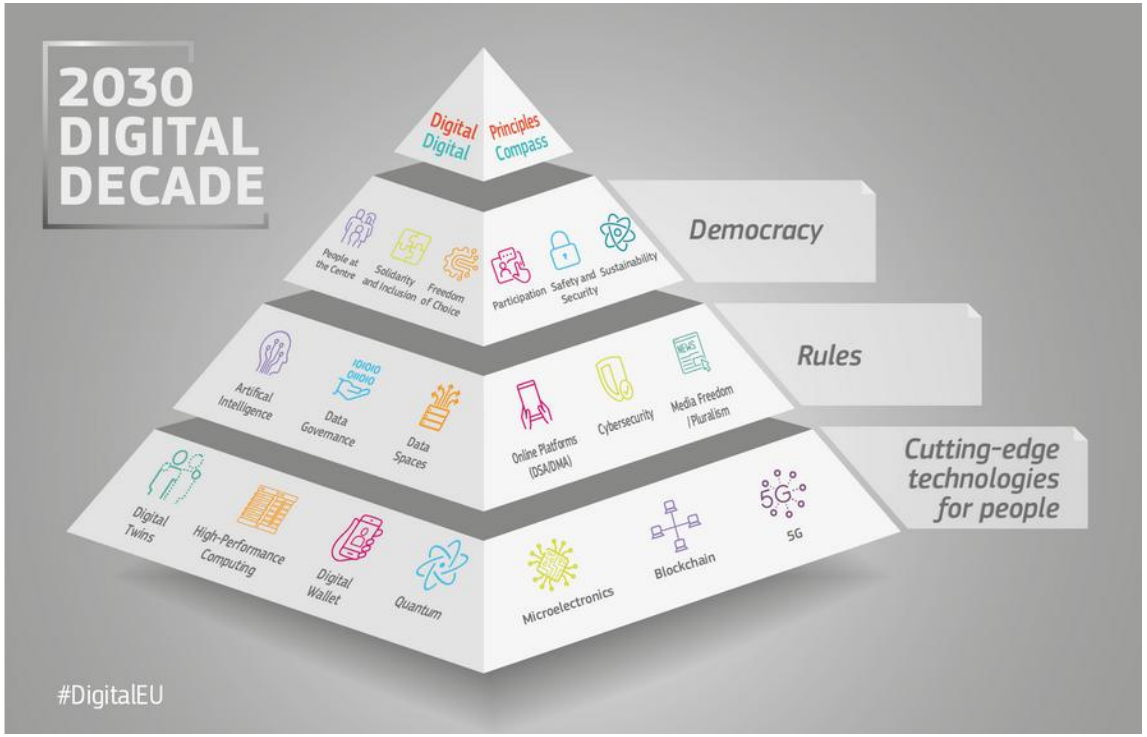
- En cas de violation fréquente des obligations de cybersécurité, les Etats membres pourront prévoir des **sanctions d'ordre pénal**

* En France, l'ANSSI exerce les fonctions de conseil et de superviseur.

Le projet de loi de transposition de NIS 2 prévoit que, concernant les sanctions, l'organe compétent sera la **Commission des sanctions** : indépendante, composée de magistrats du Conseil d'État, de la Cour de cassation et de la Cour des comptes, ainsi que de personnalités qualifiées.

DORA : pour un secteur financier cyber-résilient

Décennie numérique de l'UE



Un Règlement et une Directive (2022)

Novembre 2022, adoption :

- **Règlement DORA ➔ qui s'applique depuis le 17/01/2025**

Objectif : renforcer et harmoniser la gestion des risques liés aux technologies de l'information et de la communication (TIC) et à la sécurité des réseaux et des systèmes d'information au niveau de l'UE

- **Directive DORA ➔ en cours de transposition**

Objectif : modifier les directives existantes telles que les directives DSP2, Solvabilité 2, IORP2, MiFID 2, AIFM… afin de les mettre en cohérence avec les nouvelles dispositions du règlement DORA.

Le règlement DORA fait partie du ***Digital Financial Package (DFP)*** qui vise à développer une approche européenne harmonisée de la finance numérique. Ce paquet législatif comprend aussi la proposition sur les marchés de crypto-actifs (MiCA) et le régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués (DLT). Et il s'inscrit, plus globalement, dans la **stratégie numérique européenne**.

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 juin 2026.**

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

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**).

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*)

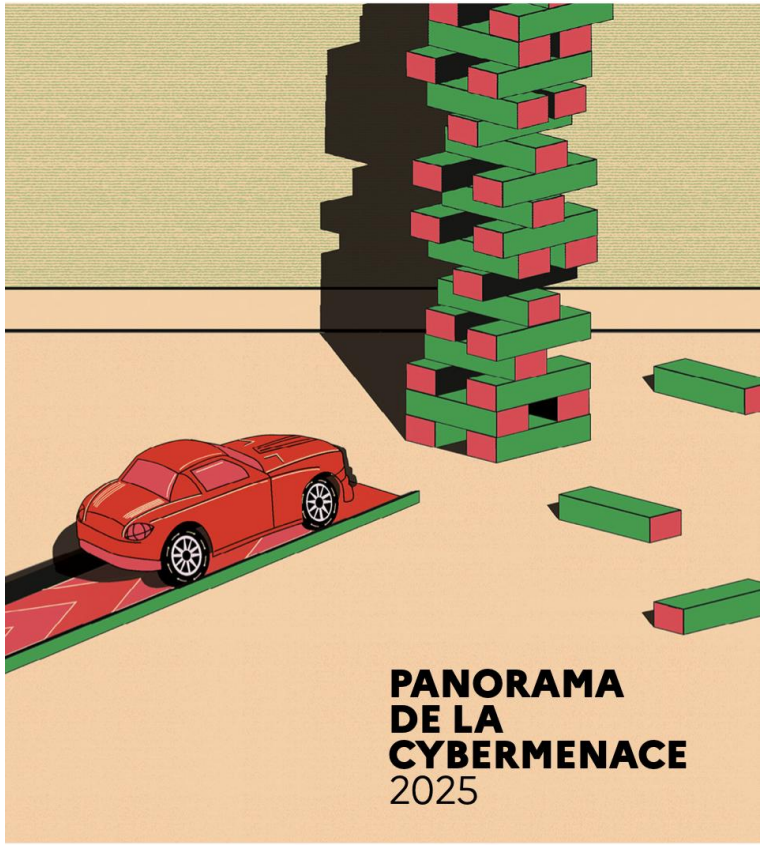
Avec ce projet de loi, la France transpose trois directives :

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

Pour aller plus loin

https://www.cert.ssi.gouv.fr/cti/CERTFR-2023-CTI-004

Rapport du ministère de l'Intérieur 2025 sur la menace



Merci de votre attention