

## À LA UNE DU MOIS : LA DIRECTIVE NIS 2

Adoptée le 14 décembre 2022, la [directive \(UE\) 2022/2555 NIS 2](#) est entrée en vigueur en France le 17 octobre 2024. En attendant la loi de transposition, nous vous présentons les principaux points clés :

**Objectifs** : la directive NIS 2 vise à renforcer la cybersécurité dans l'UE en élargissant son champ d'application par rapport à NIS 1. NIS 2 couvre désormais 18 secteurs (au lieu de quelques-uns sous NIS 1), incluant des domaines comme l'espace, l'administration publique, les denrées alimentaires et les services postaux. Cette extension vise à mieux protéger les infrastructures critiques et d'accroître la résilience globale face aux cybermenaces, en intégrant des entités de taille moyenne et grande.

**Personnes concernées** : elle s'applique aux entités publiques et privées des secteurs essentiels et importants, définis dans les annexes I et II. Cela inclut des milliers d'entités en France, des PME aux grandes entreprises.

**Principales obligations** :

- mise en place de mesures de gestion des risques de cybersécurité, en ce compris des formations obligatoires ;
- déclaration des incidents majeurs aux autorités compétentes ;
- renforcement des audits et évaluations de sécurité ;
- insertion de clauses obligatoires dans les contrats avec les sous-traitants emportant une application par effet domino de cette directive à des acteurs hors périmètre ;
- identification et enregistrement des entités concernées auprès de l'ANSSI.

**Sanctions** : les sanctions pour non-conformité peuvent atteindre 10 millions d'euros ou 2 % du chiffre d'affaires mondial pour les entités essentielles, et 7 millions d'euros ou 1,4 % du chiffre d'affaires mondial pour les entités importantes. En outre, les dirigeants peuvent être tenus personnellement responsables en cas de manquement grave à leurs obligations.

## Jurisprudence

**Appréciation du risque de confusion avec les marques de renommée (PUMA vs JAMES BOND)** : le risque de confusion dans l'esprit du public entre deux marques est un motif de nullité relative.

Dans une première affaire, l'EUIPO a reconnu un risque d'association entre "Bond Pickleball" et la marque renommée "James Bond", en raison de la réputation de cette dernière liée à un univers de luxe, même si les produits concernés étaient différents. [EUIPO, 20 déc. 2024](#).

À l'inverse, dans une seconde affaire, le Tribunal de l'UE a jugé que la marque "Li Puma Design" pour des services de recyclage ne créait pas de lien avec la marque renommée "PUMA", faute de proximité suffisante entre les secteurs. [Tribunal de l'UE, 4 décembre 2024, T-30/24](#).

Ces décisions montrent que l'appréciation du risque de confusion repose sur l'existence d'un lien mental dans l'esprit du public pertinent, influencé par la renommée de la marque et la nature des produits ou services concernés. [EUIPO, 14 janvier 2025](#)

**Chanel c/ Jonak** : l'enseigne Jonak a été condamnée pour avoir imité la célèbre paire bicolore « Slingback » de Chanel. La Cour d'appel de Paris a reconnu que Jonak avait commis des actes de parasitisme en ayant cherché à tirer indûment profit de la renommée de la maison de luxe, en se basant sur une similitude visuelle avec la combinaison beige et noir, ainsi que l'utilisation de la chaîne entrelacée caractéristique. Chanel a démontré une valeur économique individualisée de ses produits à travers des éléments de preuve significatifs. En conséquence, Jonak a été condamnée à verser 180 000 € pour préjudice économique et moral, avec interdiction de commercialiser les modèles litigieux. [CA Paris 16 octobre 2024 n° 22/19513](#)

## Bon à savoir

**Certification RGPD des sous-traitants** :

La CNIL a ouvert une consultation publique jusqu'au 28 février 2025 pour recueillir des avis sur un projet de référentiel visant à certifier les sous-traitants en matière de conformité au RGPD. Cette certification permettra d'orienter les responsables de traitement dans le choix de leurs sous-traitants : elle assure que les traitements réalisés par le sous-traitant certifié ont été évalués comme étant conformes aux critères d'un référentiel reconnu par la CNIL.

<https://www.cnil.fr/fr/certification-rgpd-des-sous-traitants-la-cnil-consulte-sur-un-projet-de-referentiel-devaluation>

**Dernières sanctions émises par la CNIL** :

- KASPR sanctionnée d'une amende de 240.000 € pour plusieurs manquements au RGPD. KASPR, qui commercialise une extension payante pour le navigateur Chrome permettant à ses utilisateurs d'accéder aux coordonnées professionnelles des personnes sur LinkedIn et d'autres sites tels que des annuaires de noms de domaine, a collecté ces données sans le consentement des intéressés pour constituer sa base de données de 160 millions de contacts. Elle n'a pas non plus respecté les droits d'information et d'accès des personnes concernées. [San-2024-020 5 décembre 2024](#)
- ORANGE sanctionnée de 50 M d'euros pour deux manquements graves :

- (i) avoir affiché des publicités entre les courriels des utilisateurs de son service de messagerie électronique sans leur consentement (cf. [les règles de prospection commerciale par courrier électronique-CNIL](#))
- (ii) le maintien de la lecture des cookies même après le retrait du consentement des utilisateurs, en violation de l'article 82 de la loi Informatique et Libertés. [SAN-2024-019 14 novembre 2024](#)

La directive sur les produits défectueux entrera en vigueur le 9 décembre 2026 et abrogera la directive 85/374/CEE, sous réserve d'une loi de transposition.

L'évolution de cette directive prévoit d'étendre le champ d'application des produits physiques à tous les systèmes numériques, dont l'IA, sauf les logiciels libres.

**Le texte responsabilise tous les opérateurs économiques** : la directive étend la responsabilité au-delà du fabricant traditionnel. Elle inclut désormais le fabricant de composants, l'importateur, et tout acteur contribuant à modifier substantiellement un produit. En l'absence de ces entités, le distributeur ou le fournisseur de services en ligne peut également être tenu responsable. Cette extension vise à assurer qu'au moins une entité peut être tenue responsable des dommages causés par des produits défectueux.

**Pour aider les victimes dans leurs démarches juridiques**, la directive introduit plusieurs présomptions facilitant la preuve de la défectuosité et/ou du lien de causalité entre le défaut et le dommage. Par exemple, la défectuosité peut être présumée en cas de dysfonctionnement manifeste du produit. De plus, les demandeurs peuvent demander aux juridictions d'ordonner la divulgation de preuves pertinentes, renforçant ainsi leur accès aux informations nécessaires pour établir leur cause. Ces mesures prennent en compte la complexité technique des nouveaux produits, notamment ceux liés aux technologies innovantes.

[Directive \(UE\) 2024/2853 du 23 octobre 2024](#)

Avec le règlement sur l'intelligence artificielle, ce corpus est destiné à garantir l'indemnisation des victimes d'un dommage causé par des produits ou services liés à une IA.