CRA : Comment se mettre en conformité ?

Les essentiels à retenir

JUIN 2026

Mathias Avocats

Mathias | Avocats

AVIS IMPORTANT

Les informations contenues dans le présent document ne constituent pas des conseils juridiques et ne peuvent s'y substituer.

Cyber Resilience Act : pour la sécurité des produits connectés

Quel contexte ?

Les **entités telles utilisent de nombreux objets connectés au sein de leurs activités quotidiennes**.

Toutefois, un certain nombre de ces produits présentent des **normes de sécurité insuffisantes, constituant ainsi une cible pour les cyberattaques**. Ces **attaques peuvent avoir de graves conséquences sur le fonctionnement de ces entités** (perte de chiffre d'affaires, atteinte réputationnelle etc.).

Face à cet enjeu, le CRA permet de **s'assurer que les fabricants proposent des produits présentant un niveau de cybersécurité plus élevé, et ce, tout au long de la vie des produits**.

Cette législation répond à une prise de conscience croissante des vulnérabilités auxquelles sont exposés les utilisateurs dans un monde de plus en plus interconnecté.

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).

Il comprend des exceptions : SaaS, secteur médical, aviation…

Objectifs

- Améliorer la **sécurité des produits comportant des éléments numériques** dès la phase de conception/développement et tout au long du cycle de vie ;
- Mettre en place un **cadre cohérent** au niveau de l'UE en matière de cybersécurité ;
- Améliorer la **transparence** sur la sécurité des produits ; et
- Permettre aux **entreprises** et aux **consommateurs** d'utiliser les produits comportant des éléments numériques en toute sécurité.

Calendrier de mise en œuvre prévu dans le Règlement

Le Cyber resilience Act est adopté

Entrée en application des principales mesures

23/11/2024	11/06/2026	11/09/2026	11/12/2027	3 ans après entrée en vigueur du CRA (puis tous les 4 ans)
	Dispositions relatives à la notification des organismes d'évaluation de la conformité (Chapitre IV, article 34 à 51)	Obligations en matière de communication d'informations / signalements incombant aux fabricants (article 14)	Entrée en application des autres dispositions du CRA	*La Commission fournira au Parlement un rapport d'audit concernant la bonne mise en œuvre et application du CRA*

Exemption d'application du CRA (non-exhaustif)

Article 69§2 du CRA

« Les produits comportant des éléments numériques qui ont été mis sur le marché avant le 11 décembre 2027 ne sont soumis aux exigences énoncées dans le présent règlement que si, à compter de cette date, ces produits font l'objet d'une modification substantielle ».

Bonne démarche : Identifier, cartographier vos produits qui font l'objet d'une «*modification substantielle*».

Article 3§30 du CRA : *« une modification apportée au produit comportant des éléments numériques à la suite de sa mise sur le marché, qui a une incidence sur la conformité du produit comportant des éléments numériques aux exigences essentielles de cybersécurité énoncées à l'annexe I, partie I, ou qui entraîne une modification de l'utilisation prévue pour laquelle le produit comportant des éléments numériques a été évalué ».*

Quel est votre niveau de maturité ?

Actions entreprises	Statut
1. Évaluation de l'application du CRA à votre entité.	OUI/NON
2. Évaluation des produits concernés par le CRA et/ou ceux soumis à une « modification substantielle».	OUI/NON
3. Qualification de votre entité (fabricant, distributeur, etc.) et identification des produits concernés par le CRA.	OUI/NON
4. Absence de formalisation et de mise en œuvre d'un plan de mise en conformité au CRA.	OUI/NON
5. Formalisation et mise en œuvre d'un plan de mise en conformité au CRA.	OUI/NON
6. Mise à jour des contrats en cours.	OUI/NON

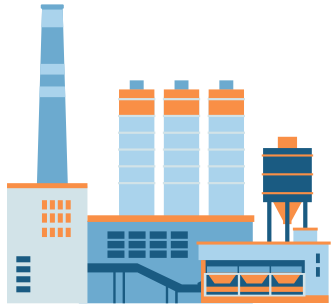
Quelles principales étapes à suivre pour se mettre en conformité ?

Évaluer l'application du CRA à mon entité et/ou ses impact sur cette dernière.

Opérer une qualification de mon entité (fabricant, fournisseur, utilisateur,etc.), ainsi qu'une qualification des produits (produits importants comportant des élements numérique etc.).

Identifier les obligations du CRA applicable à mon entité au regard de sa qualification ainsi qu'au regard de la qualification des produits.

Mettre en place une gouvernance adaptée.



Quelles sont les principales obligations du fabricant ? (non-exhaustives)

Distribution et sécurité des mises à jour.

Identifier et documenter les vulnérabilités.

Obligations de communication (découverte de vulnérabilités ou incidents graves).

Formaliser la documentation technique.

Établir la déclaration UE de conformité.

Apposer le marquage CE.

Le fabricant doit également intégrer la sécurité dès la conception (security by design).

Quelles sont les principales obligations de l'importateur ? (non-exhaustives)

Vérifier la conformité avant la mise sur le marché.

Conserver la documentation et la déclaration de conformité pendant au moins 10 ans.

Refuser la mise sur le marché de produits non conformes.

Signaler tout risque de cybersécurité au fabricant et aux autorités.

Quelles sont les principales obligations du distributeur? (non-exhaustives)

S’assurer que le fabricant et l’importateur ont respecté leurs obligations (traçabilité, information, conformité, documentation).

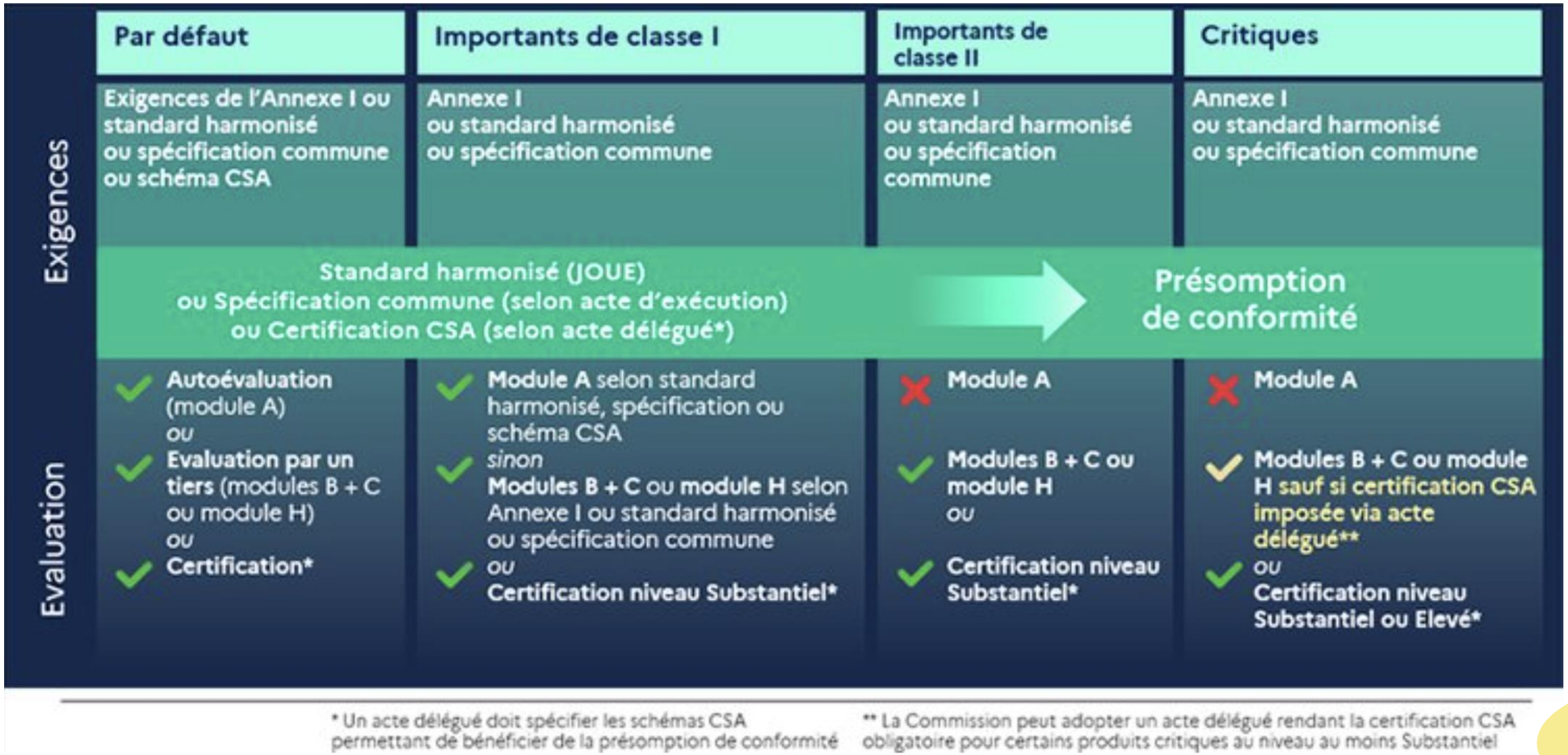
Refuser la distribution de produits non conformes.

Informer sans délai le fabricant et les autorités en cas de risque ou de vulnérabilité grave.

Participer aux mesures correctives (retrait, rappel, mise en conformité).

Quel principal enjeu lié à la qualification du produit ?

La qualification du produit pour l'évaluation de la conformité des produits comportant des éléments numériques incombe au fabricant.



Source : ANSSI

Quelle gouvernance mettre en place ?

En tant que fabricant, notamment :

Effectuer des audits de sécurité.

Formaliser, conserver et mettre à jour la documentation technique : impliquer les équipes juridiques, de conformité et de développement.

Formaliser une procédure d'urgence pour la notification d'incidents graves de sécurité et de vulnérabilités.

Auditer et sélectionner les fournisseurs de composants (matériels ou logiciels) sur la base de critères de sécurité stricts, afin de prévenir l'importation de vulnérabilités dans le produit final.

Effectuer une mise à jour des contrats.

Quelle gouvernance mettre en place ?

En tant que distributeur/importateur, notamment :

Conserver la documentation technique permettant de démontrer la conformité du produit au CRA.

Élaborer un plan de continuité/gestion de crise incluant des procédures pour le retrait de marché et les campagnes de rappel.

Effectuer une mise à jour des contrats en y intégrant des clauses CRA.

Mettre en place une procédure de vérification de la conformité du produit avant sa mise sur le marché.

Pour le distributeur : existence du marquage CE, existence d'informations et d'instructions destinées à l'utilisateur, existence de la déclaration UE de conformité etc.)

Pour l'importateur : existence d'une procédure d'évaluation de la conformité, de la documentation technique, etc.)

Quelle gouvernance mettre en place ?

En tant qu'utilisateur, notamment :

Identifier les dépendances de l'entité (fournisseurs), ainsi que la qualification de l'entité au regard du CRA (fabriquant ? Importateur ? Etc.).

Mise en place d'un processus de *due dilligence* (Intégrer les questionnaires fournisseurs ainsi que des grilles d'évaluation de ces derniers dans les appels d'offre et dans les contrats, etc.).

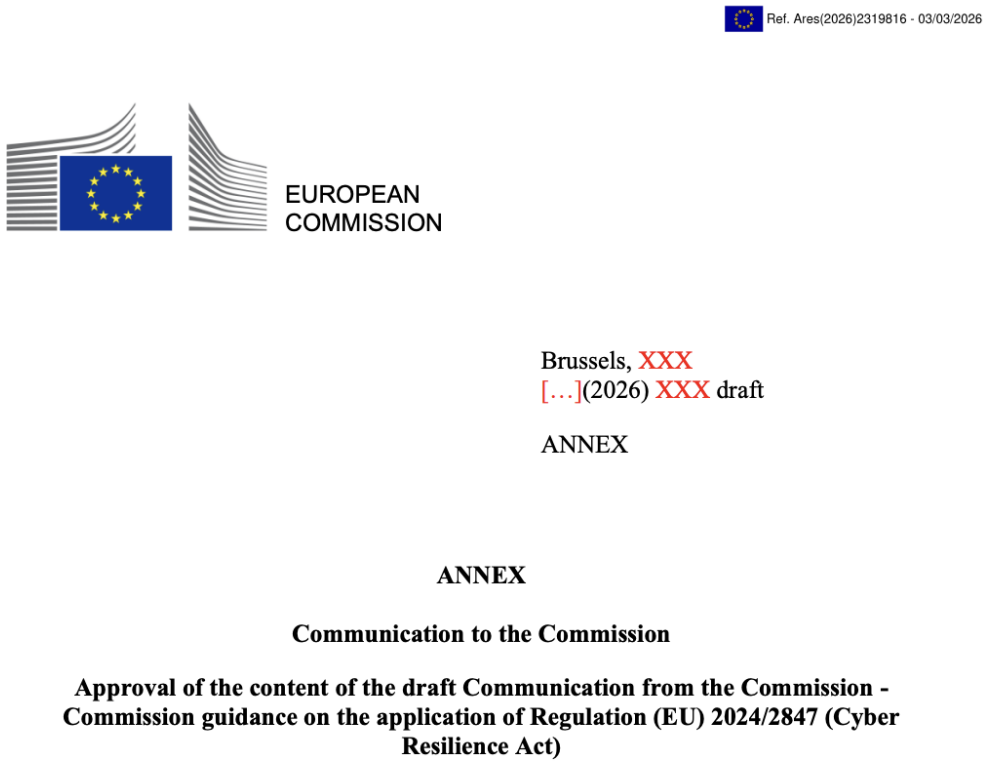
Cartographier l'ensemble des produits comportant des éléments numériques.

Intégrer les critères du CRA dans la politique globale de gestion des risques liés aux tiers.

Publication d'un projet d'orientation par la Commission européenne

La Commission européenne a publié le 3 mars 2026 un **projet** d'orientations, ayant pour objectif d'aider les entreprises à respecter les obligations issues du CRA.

Ce projet vise notamment à préciser le champ d'application des dispositions du CRA, en accordant une attention particulière à la simplification de leur mise en conformité pour les microentreprises ainsi que pour les petites et moyennes entreprises.



Ref. Ares(2026)2319816 - 03/03/2026

EUROPEAN COMMISSION

Brussels, XXX
[…](2026) XXX draft

ANNEX

ANNEX

Communication to the Commission

Approval of the content of the draft Communication from the Commission - Commission guidance on the application of Regulation (EU) 2024/2847 (Cyber Resilience Act)

Consulter le projet de la Commission européenne

Des formations sur-mesure pour vous et vos équipes, Contactez-nous !

FORMATIONS

Retrouvez les programmes proposés par l'organisme de formation Mathias Avocats

Qualiopi processus certifié
RÉPUBLIQUE FRANÇAISE
La certification qualité a été délivrée au titre de la ou des catégories d'actions suivantes :
Actions de formation

Retrouvez l'intégralité du Catalogue des formations

Conformité | Cyber Resilience Act – CRA | Cybersécurité

Cyber Resilience Act (IoT) : L'essentiel pour maîtriser les enjeux clés et réussir votre mise en conformité

4 heures, en présentiel - continu

Télécharger
293,55 Ko - pdf

Cybersécurité

Aspects juridiques de la cybersécurité: Fondements, obligations et gestion des risques

Durée : 4 heures, en présentiel - continu

Télécharger
240,77 Ko - pdf

Cybersécurité

Gestion de crise, réponse à incident : L'essentiel pour maîtriser les principes clés et réussir votre mise en conformité

Durée : 4 heures, en présentiel - continu

Télécharger
245,67 Ko - pdf

MATHIAS Avocats

20 ans d'expertise en droit du numérique

Mathias | Avocats

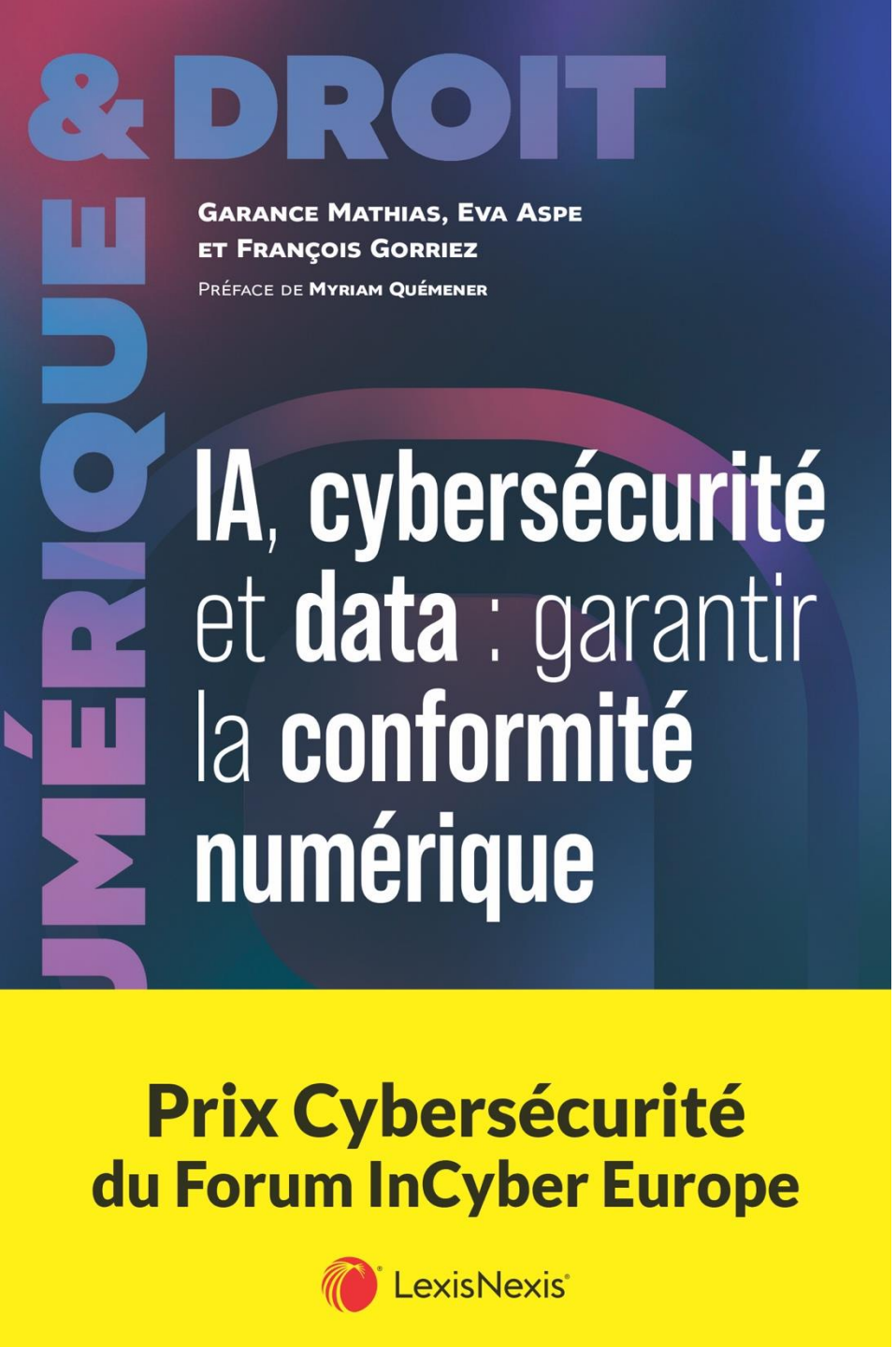
Besoin d'une veille juridique sur mesure ?

Sur les thématiques qui vous intéressent, sur votre secteur d'activité, votre métier, les nouvelles exigences / le cadre juridique de vos missions, vos opportunités…

NOUS CONTACTER

Mathias Avocats réalise des veilles sur-mesure pour ses clients, selon les thématiques sélectionnées, secteurs d'activités, métiers.

- **Une veille pour vous et vos équipes, chaque mois dans votre boîte mail**
- **Contenu, format, périodicité, tarif : contactez-nous !**



Pour vous et vos équipes !

Disponible chez votre libraire (ou achat en ligne)

LexisNexis

Cet ouvrage décrypte les réglementations (***NIS 2, DORA, AI Act, Data Act, Cyber Resilience Act, etc***.) pour vous permettre de maîtriser les risques juridiques, de la contractualisation à la gestion de crise et à sa remédiation, en intégrant également la R&D et l'innovation.

Il contient des **schémas, infographies, interviews de professionnels** (dirigeants, responsables cybersécurité, conformité IA, data, etc.), **des recommandations et outils** (notamment des **« check-lists » de questions à se poser, des points de vigilance** sur les **contrats** et la **gestion de crise**).

Conçu comme un **guide pratique**, cet ouvrage propose un parcours de conformité en 5 étapes-clés : **Gouverner, Concevoir, Contractualiser, Gérer les crises et Anticiper**, qui vous accompagnera pour piloter votre conformité numérique.

Par Garance MATHIAS, Eva ASPE et François GORRIEZ,
Editions LexisNexis, Janvier 2026.

Mathias | Avocats

SUIVEZ VOTRE ACTUALITÉ, ABONNEZ-VOUS !

UNE NEWSLETTER MENSUELLE OFFERTE

Mathias | Avocats

JANVIER 2026

Newsletter

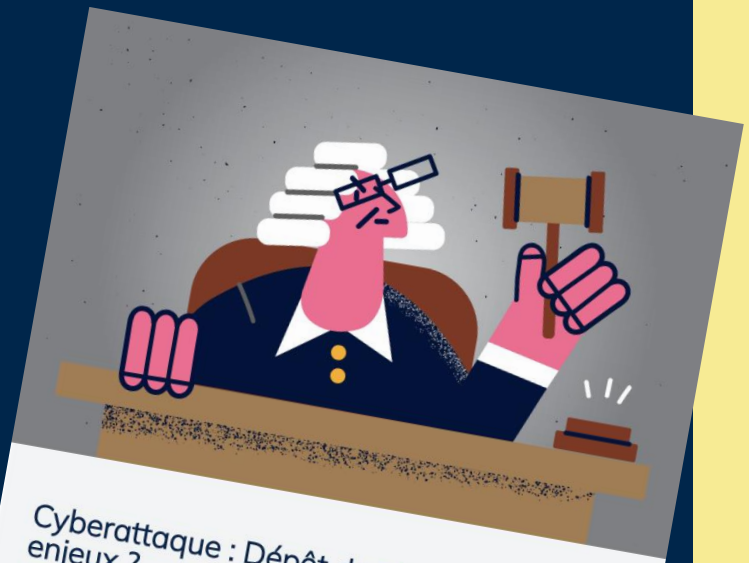
VOUS AVEZ PEUT-ÊTRE MANQUÉ...

Déploiement d'outils d'IA dans l'entreprise : le rôle du CSE

L'introduction de nouvelles technologies, dont l'IA, au sein des entreprises nécessite la consultation et l'information du Comité Social et Economique (CSE) dès lors que cette nouvelle technologie peut modifier les conditions de travail (article L 2312-8 du code du travail).

Quelles sont les bonnes pratiques lors du déploiement d'outils d'IA ? Quels sont les apports de décisions de justice récentes concernant le rôle, à cet égard, du CSE ?

EN SAVOIR PLUS



Cyberattaque : Dépôt de plainte, quels enjeux ?

24 Avr, 2026 | Contentieux, Cybersécurité / Cybercriminalité

Dans un contexte d'intensification de la menace cyber, la phase contentieuse n'est pas qu'une riposte en cas de cyberattaque. Les enseignements tirés des poursuites et des décisions judiciaires nourrissent la stratégie de conformité et renforcent la...

lire plus

L'ACTUALITÉ DÉCRYPTÉE POUR VOUS !

ENSEMBLE, DÉVELOPPONS VOS PROJETS
ET FORMONS VOS ÉQUIPES !
PARTAGEONS NOS EXPERTISES !

AU QUOTIDIEN

Catalogue des formations

Mathias | Avocats

CONTACTEZ-NOUS !

19 rue Vernier 75017 PARIS

+33 (0)1 43 80 02 01

contact@avocats-mathias.com

https://www.avocats-mathias.com/

@MathiasAvocats