

Newsletter

Tech / Data

3e Trimestre 2026

AI Act : les nouvelles obligations de transparence sur les contenus générés par l'IA sont applicables

Depuis le 2 août 2026, l'article 50 de l'AI Act impose de nouvelles obligations de transparence concernant les contenus générés ou manipulés par l'intelligence artificielle. Les entreprises doivent notamment informer le public de l'utilisation de certains contenus synthétiques, tels que les deepfakes, sous peine de sanctions pouvant atteindre 15 millions d'euros ou 3 % du chiffre d'affaires annuel mondial.

Dans ce numéro

Amende de 2,33 millions d'euros pour Boohoo : prix barrés et mentions de composition trompeuse **3**

Signalement de vidéos à YouTube : la demande de blocage fondée sur un contenu non contrefaisant engage la responsabilité de son auteur **4**

Loi anti-« ultra fast fashion » : une interdiction de promotion pour les influenceurs à compter du 1er janvier 2027 **5**

Retrait de contenus sur Instagram : le juge distingue les contenus menaçants ou harcelants des accusations diffamatoires **6**

AI Act : ce que change l'article 50 en matière de transparence des contenus générés par l'IA **7**

Adoption de la réforme du code des douanes de l'Union : un rôle accru pour les plateformes de e-commerce **8**

France Travail : 5 millions d'euros d'amende pour des défauts de sécurité identifiés mais non corrigés à temps **9**

ChatGPT, Reddit et Roblox désignés au titre du DSA : des obligations renforcées d'ici la fin de l'année **10**

Démarchage téléphonique : le consentement préalable devient la règle depuis le 11 août 2026 **11**

Première notification d'une violation de données imputée à un agent d'intelligence artificielle	12
---	-----------

Breaking news AI Act : premières demandes formelles d'informations du Bureau européen de l'IA aux fournisseurs de modèles	12
---	-----------

Uber sanctionné à hauteur de 824,99 millions d'euros pour des décisions automatisées de désactivation de comptes	13
--	-----------

Cyberattaque à l'Hôpital privé de la Loire : 500 000 euros d'amende pour des manquements à la sécurité des données de santé	14
---	-----------

Concurrence déloyale : la détention d'informations confidentielles sur l'ordinateur d'un ancien salarié caractérise leur appropriation par le nouvel employeur	15
--	-----------

ACTUALITES NOUVELLES TECHNOLOGIES



Amende de 2,33 millions d'euros pour Boohoo : prix barrés et mentions de composition trompeuse

Le 20 août 2026, la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) a annoncé que le site britannique de vente de vêtements Boohoo avait accepté de payer, dans le cadre d'une transaction pénale, une amende de 2,33 millions d'euros. Cette sanction fait suite à une enquête portant sur les prix de plusieurs centaines de produits.

Les agents de la DGCCRF ont relevé des pratiques commerciales trompeuses sur la réalité des promotions annoncées : certains prix étaient majorés avant l'application de la promotion, de manière à en gonfler artificiellement l'ampleur, et d'autres promotions précédemment appliquées n'étaient pas prises en compte. Au total, 95 % des annonces contrôlées étaient non conformes : quatre sur dix n'offraient aucune baisse de prix, 7 % une baisse moins importante que celle annoncée, et près de la moitié correspondaient en réalité à une augmentation de prix.

Ces agissements relèvent de la pratique commerciale trompeuse, définie à l'article L. 121-2 du Code de la consommation, notamment lorsqu'elle repose sur des indications fausses ou de nature à induire en erreur portant sur le prix ou son caractère promotionnel. Les annonces de réduction de prix sont par ailleurs encadrées par l'article L. 112-1-1 du même code, qui impose au professionnel d'indiquer le prix antérieur pratiqué avant l'application de la réduction. L'article L. 132-2 du Code de la consommation sanctionne les pratiques commerciales trompeuses d'une peine de deux ans d'emprisonnement et d'une amende pouvant aller jusqu'à **300 000 euros ou 10 % du chiffre d'affaires annuel moyen**.

L'enquête a également mis en évidence des manquements relatifs à la composition des produits textiles et chaussants : les termes « cuir » ou « daim » étaient employés pour désigner des produits synthétiques, et certaines informations étaient non conformes ou incomplètes.

- Cette affaire rappelle que le prix barré, le pourcentage de réduction et les mentions relatives à la composition des produits constituent des informations commerciales susceptibles d'influencer la décision d'achat. Le professionnel doit pouvoir démontrer que le prix affiché, la réduction annoncée et les caractéristiques du produit correspondent à la réalité.

ACTUALITES NOUVELLES TECHNOLOGIES

Signalement de vidéos à YouTube : la demande de blocage fondée sur un contenu non contrefaisant engage la responsabilité de son auteur

Tribunal judiciaire de Paris, 3e chambre 2e section, 19 juin 2026, n° RG 24/03517

Par un jugement du 19 juin 2026, le Tribunal judiciaire de Paris condamne une société de production à verser 22 000 euros de dommages et intérêts pour avoir obtenu le blocage de vidéos sur YouTube alors que celles-ci n'étaient pas illicites.

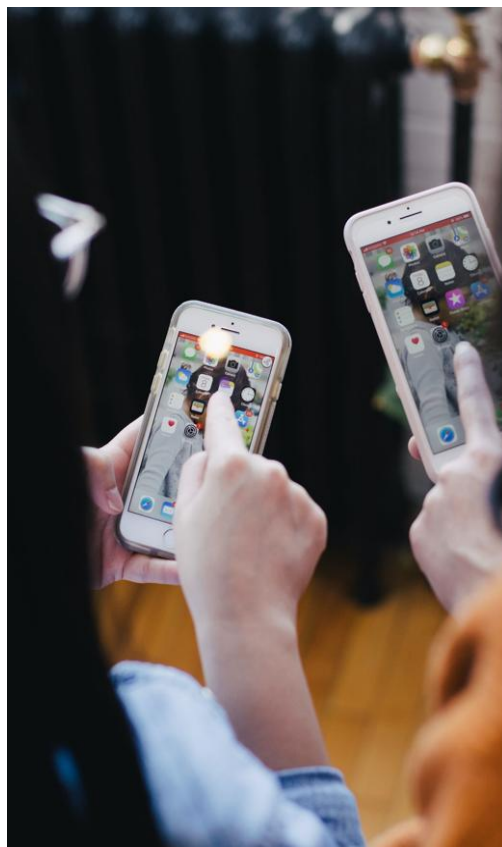
Le producteur, l'auteur et le réalisateur de l'émission « Les Incorrectibles » reprochaient à l'association Observatoire du conspirationnisme d'avoir intégré, dans le générique de son programme « Les Décons-pirateurs », des extraits de deux secondes issues de deux de leurs émissions. Ils invoquaient la contrefaçon de droits d'auteur et, subsidiairement, la concurrence déloyale. La société de production avait par ailleurs demandé le blocage des vidéos de l'association sur YouTube, 22 vidéos étant devenues indisponibles à compter de février 2024.

Le tribunal écarte d'abord la contrefaçon. Le décor (une banquette sur fond uni), la position des interlocuteurs et l'alternance de plans larges et serrés relèvent selon lui du fonds commun des interviews télévisées : leur combinaison ne procède que d'un assemblage d'éléments banals, ne révélant pas de choix libres et créatifs. Le format d'émission et les deux émissions concernées ne sont donc pas protégés par le droit d'auteur. Faute d'œuvre protégée, le tribunal n'examine pas l'exception de courte citation, invoquée à titre subsidiaire par l'association. La concurrence déloyale et le parasitisme sont également écartés : les extraits, d'une durée de deux secondes, servent à illustrer le propos de l'association dans un débat d'intérêt général, et le logo de l'émission reste visible.

C'est sur cette base que le tribunal juge fautive la demande de blocage. Il rappelle qu'une notification à un hébergeur n'est pas fautive par principe, puisqu'elle permet de faire cesser un contenu illicite (article 6 de la LCEN, puis articles 6 et 16 du règlement sur les services numériques). Toutefois, lorsqu'elle émane d'une personne ayant un intérêt commercial, la notification est faite aux risques et périls de son auteur : elle est fautive si elle vise une interdiction qui n'est pas justifiée, ce qui s'apprécie objectivement, au regard des règles de fond, indépendamment de la bonne foi de son auteur. Les vidéos n'étant pas contrefaisantes, elles ne pouvaient être interdites, et la société de production, qui avait un intérêt économique au blocage, engage sa responsabilité. En revanche, il n'est pas établi que l'auteur et le réalisateur, personnellement, soient à l'origine des blocages.

Le tribunal rejette la demande de réparation d'un préjudice économique de 41 200 euros, les vidéos de l'association n'étant pas monétisées. Il retient en revanche un préjudice moral, fixé à 1 000 euros par vidéo, soit 22 000 euros pour 22 vidéos bloquées depuis plus de deux ans. La demande de l'association pour procédure abusive est rejetée, et les demandeurs sont condamnés in solidum aux dépens et à lui verser 7 000 euros au titre de l'article 700 du Code de procédure civile.

- Cette décision invite à vérifier, avant tout signalement à une plateforme, le caractère illicite du contenu au regard du droit invoqué : le risque de responsabilité existe même en l'absence de mauvaise foi.



ACTUALITES NOUVELLES TECHNOLOGIES

Loi anti « ultra fast fashion » : une interdiction de promotion pour les influenceurs à compter du 1er janvier 2027

Loi n° 2026-602 du 8 juillet 2026 visant à réduire l'impact environnemental de l'industrie textile (JORF du 9 juillet 2026)

La loi n° 2026-602 du 8 juillet 2026 visant à réduire l'impact environnemental de l'industrie textile a été promulguée le 8 juillet 2026 et publiée au Journal officiel du 9 juillet 2026. Elle introduit dans le Code de l'environnement la notion de « mode ultra-express » (article L. 541-9-1-1).

Relèvent de la mode ultra-express les pratiques industrielles et commerciales des producteurs qui diminuent la durée d'usage ou la durée de vie des produits textiles, en raison de la mise sur le marché d'un nombre élevé de références de produits neufs et de la faible incitation à réparer ces produits. Ces deux éléments sont cumulatifs. Lorsqu'une interface en ligne (place de marché, plateforme) permet la vente à distance de ces produits, la pratique est appréciée dans les mêmes conditions. Les seuils relatifs au nombre de références et les critères de la faible incitation à réparer, par marque et par canal de vente, seront fixés par décret en Conseil d'État.

Pour les influenceurs, l'article 7 de la loi insère un IV bis à l'article 4 de la loi n° 2023-451 du 9 juin 2023 sur l'influence commerciale. Il interdit à toute personne exerçant une activité d'influence commerciale par voie électronique, à titre onéreux ou gratuit et quelle que soit la contrepartie, toute promotion directe ou indirecte des produits relevant de la mode ultra-express et des marques ayant recours à cette pratique. La sanction encourue est une amende administrative pouvant atteindre 100 000 euros, prononcée dans les conditions prévues au livre V du Code de la consommation. Cette interdiction entre en vigueur le 1er janvier 2027.

L'article 6 interdit plus largement la publicité relative aux produits de la mode ultra-express ou faisant la promotion directe ou indirecte des marques ayant recours à cette pratique (article L. 229-61-1 du Code de l'environnement). Pour ces produits, le terme « gratuit » ne peut plus être utilisé comme outil de marketing ou de promotion.

La loi comporte d'autres mesures, notamment l'obligation pour les plateformes concernées d'afficher des messages encourageant la sobriété, le réemploi et la réparation, l'affichage des lieux de fabrication à proximité du prix pour les produits vendus en ligne, et une modulation des contributions des producteurs à l'éco-organisme pouvant prendre la forme de pénalités par produit.

Reste la question centrale des enseignes concernées. Elle dépendra du décret en Conseil d'État, qui fixera les seuils et critères applicables par marque et par canal de vente. Les influenceurs ne pourront plus promouvoir les marques qui en relèveront à compter du 1er janvier 2027.



ACTUALITES NOUVELLES TECHNOLOGIES

Retrait de contenus sur Instagram : le juge distingue les contenus menaçants ou harcelants des accusations diffamatoires

Tribunal judiciaire de Paris, procédure accélérée au fond, 31 août 2026, n° RG 26/53322



Par un jugement du 31 août 2026, le Président du Tribunal judiciaire de Paris précise les contenus dont un hébergeur peut se voir demander le retrait. Une agence de booking et deux DJs visaient Meta Plat-forms Ireland, hébergeur d'Instagram, afin d'obtenir la suppression d'un compte suivi par plus de 57 000 abonnés et de ses publications (menaces de mort, harcèlement, photomontages, divulgation d'une adresse, accusations d'abus sexuels), que leurs signalements à Instagram n'avaient pas fait retirer.

Le juge rappelle le cadre. Une mesure de retrait ne peut être ordonnée que si elle est justifiée par le dommage, nécessaire et proportionnée au regard de la liberté d'expression et du droit à la vie privée de l'auteur des propos. Lorsque l'action oppose la personne visée à l'hébergeur et non à l'auteur du contenu, aucun débat contradictoire n'a lieu sur la réalité de l'atteinte : seul un contenu manifestement illicite peut alors justifier un retrait, même partiel.

Ce qui est admis : les menaces et le harcèlement. Le juge retient que les stories à tonalité menaçante et harcelante, qui émaillent l'ensemble du compte, étaient susceptibles de caractériser notamment des menaces de mort, du cyberharcèlement, du doxing et des photomontages non signalés, et que leur suppression était justifiée. Meta les ayant retirées en cours de procédure, la demande est déclarée sans objet et Meta est condamnée aux dépens, la demande ayant été fondée et n'ayant abouti qu'après l'assignation.

Ce qui est refusé : le retrait des accusations d'abus sexuels. Ces imputations sont susceptibles de constituer des diffamations publiques, mais leur caractère diffamatoire ne suffit pas à les rendre manifestement illicites : la diffamation peut être écartée si la preuve de la vérité est rapportée ou si l'excuse de bonne foi est admise. Le juge relève que, malgré les motivations de riposte de l'auteur du compte, les circonstances n'excluent pas que ces révélations soient fondées, et leur retrait ne peut être ordonné tant que leur auteur n'a pas pu se défendre. Sont également rejetées la suppression de l'intégralité du compte, au risque d'atteindre du contenu licite, et la demande de filtrage par mots-clés, trop large et qui aurait rendu inaccessibles des contenus dont la suppression n'est pas permise. Les demandes relatives à deux autres comptes sont rejetées faute de pièces permettant d'établir la matérialité des contenus.

- En pratique, l'action contre la plateforme permet de faire supprimer les contenus manifestement illicites, tels que les menaces et le harcèlement, mais pas les accusations diffamatoires : une procédure contre l'auteur des propos reste nécessaire dans ce dernier cas.

ACTUALITES NOUVELLES TECHNOLOGIES

AI Act : ce que change l'article 50 en matière de transparence des contenus générés par l'IA

Règlement (UE) 2024/1689 du 13 juin 2024 (AI Act)



L'article 50 de l'AI Act est applicable depuis le 2 août 2026. Il ne se limite pas à une obligation d'étiquetage : il instaure un régime de transparence qui distingue les fournisseurs et les déployeurs de systèmes d'IA.

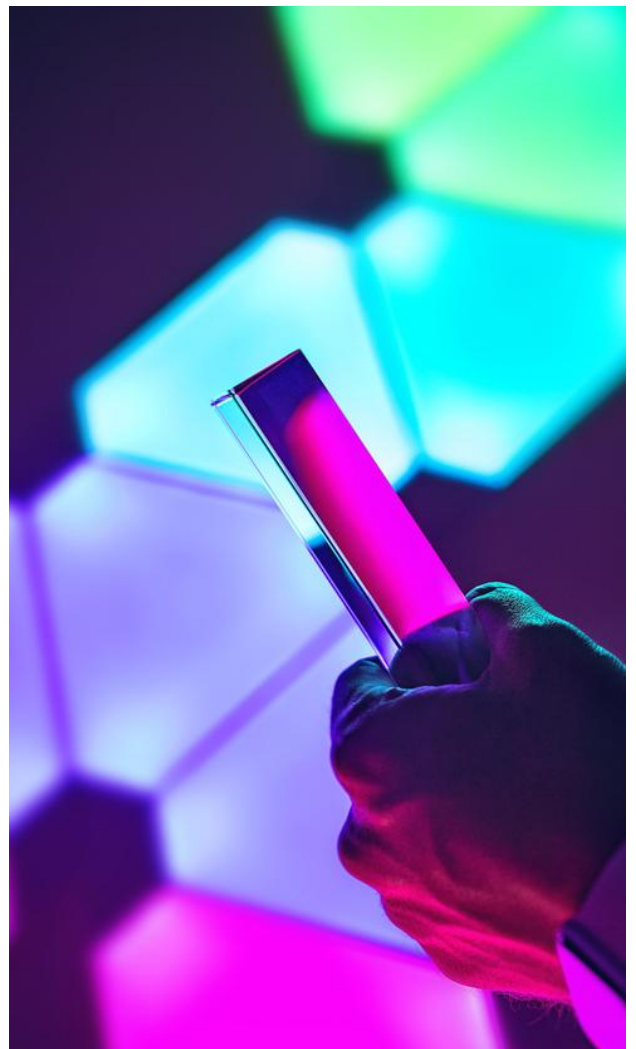
Les fournisseurs doivent intégrer un marquage lisible par machine permettant d'identifier les contenus synthétiques, de manière effective, interopérable et robuste. Cette obligation concerne les contenus textuels, sonores, visuels ou audiovisuels générés par IA, mais exclut les simples fonctions d'assistance et les modifications non substantielles.

Les entreprises utilisatrices, qualifiées de déployeurs, doivent quant à elles procéder à une divulgation visible dans deux hypothèses principales : lorsqu'elles diffusent un « deepfake », c'est-à-dire un contenu donnant faussement l'apparence d'une personne, d'un objet, d'un lieu ou d'un événement authentique, et lorsqu'elles publient un texte généré ou manipulé par IA afin d'informer le public sur une question d'intérêt général, sans contrôle humain ni responsabilité éditoriale sur son contenu.

Trois enseignements peuvent en être tirés. Le marquage technique incombe au fournisseur, tandis que le signalement perceptible par le public relève du déployeur, ce qui suppose une articulation contractuelle et technique entre l'éditeur de l'outil, l'entreprise utilisatrice, ses agences et les plateformes de diffusion. L'existence d'un véritable contrôle éditorial humain conditionne l'obligation de transparence pour les textes d'intérêt général. Enfin, la conformité suppose de pouvoir en rapporter la preuve : identifier les outils employés, retracer le processus de génération, mesurer l'intervention humaine, qualifier le contenu et déterminer qui supporte l'obligation.

Les sanctions peuvent atteindre **15 millions d'euros ou 3 % du chiffre d'affaires annuel mondial**.

- Les entreprises qui utilisent déjà l'IA ont donc intérêt à cartographier leurs usages et à documenter leur gouvernance éditoriale et le partage de responsabilité au sein de leurs contrats.



ACTUALITES NOUVELLES TECHNOLOGIES

Adoption de la réforme du code des douanes de l'Union : un rôle accru pour les plateformes de e-commerce

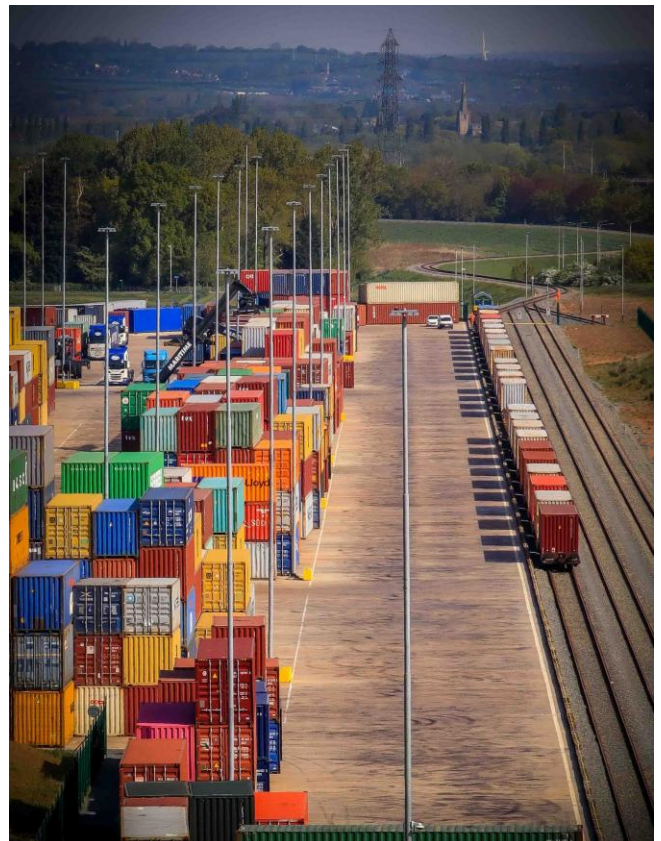
Parlement européen, résolution législative du 16 septembre 2026, P10 TA(2026)0290 (procédure 2023/0156(COD))

Le 16 septembre 2026, le Parlement européen a approuvé, en deuxième lecture, la position du Conseil sur le règlement établissant le code des douanes de l'Union et l'Autorité douanière de l'Union européenne, et abrogeant le règlement (UE) n° 952/2013. L'acte est ainsi adopté conformément à la position du Conseil. Il doit être signé puis publié au Journal officiel de l'Union européenne, et entrera en vigueur le lendemain de sa publication, les nouvelles règles étant pleinement applicables après une période de douze mois.

Cette réforme répond à l'augmentation du nombre de colis expédiés depuis des pays tiers directement aux consommateurs européens. Elle renforce l'implication des plateformes dans les formalités douanières : les vendeurs et plateformes établis dans l'Union, ou disposant du statut d'opérateur économique agréé ou d'opérateur de confiance, qui vendent à distance des marchandises de pays tiers à des consommateurs européens seront considérés comme des importateurs. Ils devront transmettre les données requises aux autorités douanières, acquitter ou garantir le paiement des droits et charges applicables, et veiller à la conformité des marchandises. En cas de manquements répétés, ils s'exposeront à une amende comprise entre 1 % et 6 % de la valeur des marchandises importées dans l'Union au cours des douze mois précédents, ainsi qu'à une suspension ou un retrait de leurs statuts douaniers.

La réforme institue également un droit de traitement applicable aux marchandises commandées auprès de boutiques en ligne de pays tiers et expédiées directement aux consommateurs européens. Son montant sera fixé par la Commission européenne et révisé tous les deux ans, et les États membres devront commencer à le percevoir au plus tard le 1er novembre 2026. Ce droit peut être réduit sous certaines conditions.

Elle prévoit enfin la mise en place de l'EU Data Hub, système informatique destiné à centraliser et exploiter les données nécessaires aux opérations douanières, qui doit remplacer au moins 111 systèmes informatiques actuellement utilisés par les autorités douanières européennes. Son utilisation sera facultative à partir de 2031 et deviendra obligatoire à compter de 2034. Un régime « Trust and Check » est par ailleurs créé pour les entreprises respectant les règles douanières et coopérant de manière transparente avec les autorités : elles bénéficieront de contrôles moins fréquents et d'une plus grande souplesse de paiement, le statut d'opérateur économique agréé étant maintenu en parallèle.



ACTUALITES DONNEES PERSONNELLES



France Travail : 5 millions d'euros d'amende pour des défauts de sécurité identifiés mais non corrigés à temps

CNIL, formation restreinte, délibération n° SAN-2026-003 du 22 janvier 2026

Le 22 janvier 2026, la CNIL a infligé une amende de 5 millions d'euros à France Travail pour plusieurs défauts de sécurité que l'opérateur avait lui-même identifiés, sans les corriger à temps. Une décision qui résonne particulièrement au regard de la récente cyberattaque révélée contre la DGFIP et qui rappelle l'importance de mettre en œuvre sans délai les mesures de sécurité identifiées.

Entre le 6 février et le 5 mars 2024, des attaquants ont usurpé, par des techniques d'ingénierie sociale, plusieurs comptes de salariés des structures CAP EMPLOI, qui accédaient à l'appliquatif métier de France Travail pour l'accompagnement des demandeurs d'emploi en situation de handicap. Les données de 36 820 828 personnes ont été exfiltrées, notamment l'état civil, le numéro de sécurité sociale, l'adresse postale, les coordonnées et le statut de demandeur d'emploi. La violation a été notifiée le 8 mars 2024.

La CNIL retient quatre manquements. Le premier porte sur la robustesse de l'authentification : les comptes n'étaient verrouillés qu'après 50 tentatives infructueuses, contre 10 au maximum selon sa recommandation, sans mesure compensatoire. Ce manquement est retenu bien qu'il n'ait pas été exploité par les attaquants, la conformité s'appréciant au regard du caractère approprié des mesures et non du scénario d'attaque réalisé. Le deuxième, le plus lourd, est l'absence d'authentification multi facteur : les analyses d'impact de 2022 avaient identifié le risque et prévu un déploiement en 2023, repoussé à avril 2024. Les deux autres portent sur l'exploitation des journaux d'activité de l'appliquatif et sur les habilitations, les conseillers CAP EMPLOI pouvant consulter les données de l'ensemble des demandeurs d'emploi, ce qui excédait le strict nécessaire.

France Travail soutenait que les CAP EMPLOI, coresponsables du traitement, devaient assumer une part des mesures de sécurité. La CNIL écarte cet argument : les conventions mettaient à la charge de France Travail la sécurité technique des outils et le contrôle des habilitations, et c'est à lui qu'il revenait de piloter les mesures de sécurité de son système d'information. Elle écarte également l'argument selon lequel un établissement de ce type échapperait à l'amende : l'exclusion prévue pour les traitements « mis en œuvre par l'État » est interprétée strictement, et France Travail, doté de la personnalité morale, est financé pour un tiers seulement par l'État.

La CNIL retient une négligence grave, les analyses d'impact ayant listé les risques qui se sont matérialisés plus de deux ans plus tard. L'amende de 5 millions d'euros, pour un plafond légal de 10 millions, est assortie d'une injonction de justifier de la mise en conformité sous astreinte de 5 000 euros par jour de retard. Cette décision rappelle qu'une analyse d'impact qui identifie un risque et planifie une mesure peut se retourner contre le responsable de traitement si la mesure reste différée : tout report doit être daté, motivé et accompagné d'une mesure intermédiaire.

ACTUALITES DONNEES PERSONNELLES

ChatGPT, Reddit et Roblox désignés au titre du DSA : des obligations renforcées d'ici la fin de l'année

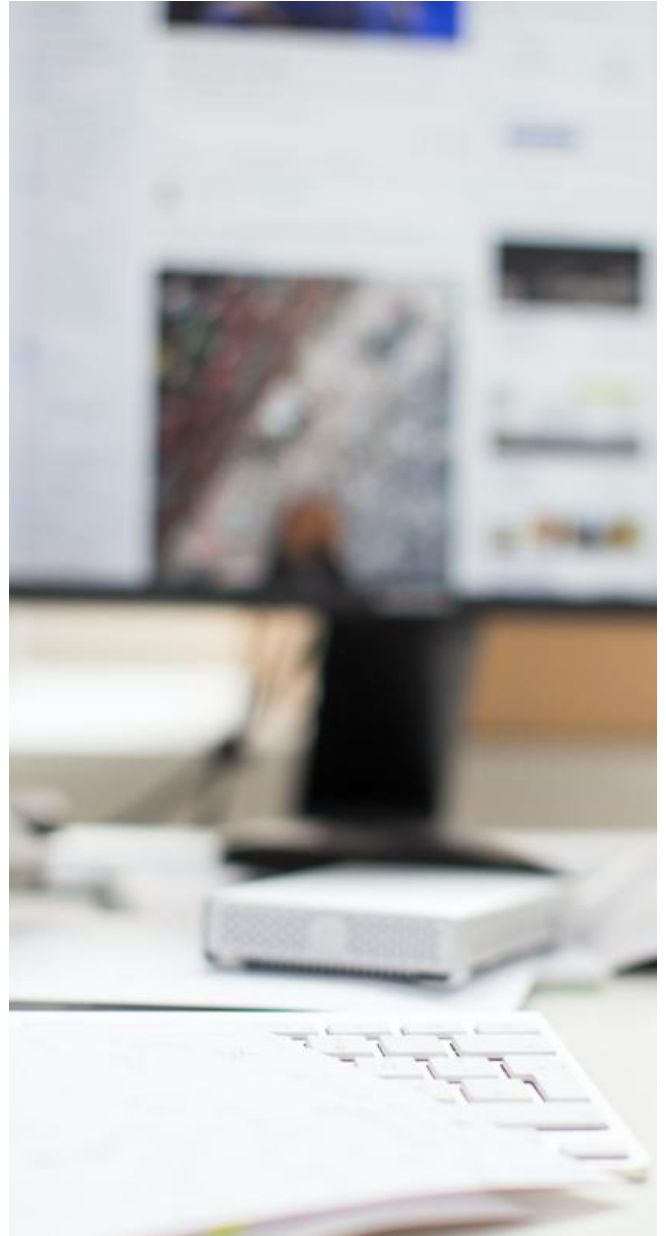
Commission européenne, règlement (UE) 2022/2065 (DSA)

Le 31 août 2026, la Commission européenne a désigné ChatGPT comme très grand moteur de recherche en ligne, une première pour un service d'intelligence artificielle, ainsi que Reddit et Roblox comme très grandes plateformes en ligne. Ces trois services déclarent chacun au moins 45 millions d'utilisateurs actifs mensuels dans l'Union, seuil à partir duquel ces règles s'appliquent.

La Commission considère ChatGPT comme un service hybride relevant de la catégorie des moteurs de recherche en ligne, dès lors qu'il peut répondre aux requêtes des utilisateurs en effectuant des recherches sur Internet.

Les trois services disposent de quatre mois, pour se conformer aux obligations supplémentaires prévues par le DSA : évaluation annuelle des risques systémiques (contenus illicites, effets sur les mineurs, santé publique, processus électoraux, droits fondamentaux), mesures d'atténuation de ces risques, audits indépendants annuels de conformité, et transparence des algorithmes de recommandation, avec une option sans profilage et un accès aux données pour les chercheurs vérifiés.

Cette désignation donne par ailleurs à la Commission des pouvoirs d'enquête lui permettant d'examiner le fonctionnement de ces services. Elle supervisera leur conformité en coopération avec le régulateur irlandais Coimisiún na Meán pour ChatGPT et Reddit, et avec l'Autorité néerlandaise des consommateurs et des marchés pour Roblox.



ACTUALITES DONNEES PERSONNELLES

Démarchage téléphonique : le consentement préalable devient la règle depuis le 11 août 2026

Loi n° 2025-594 du 30 juin 2025 contre toutes les fraudes aux aides publiques



Depuis le 11 août 2026, le démarchage téléphonique des consommateurs est interdit par principe, en application de l'article 13 de la loi n° 2025-594 du 30 juin 2025, qui modifie notamment les articles L. 221-16 et L. 223-1 et suivants du Code de la consommation.

Le régime d'opposition (« opt-out »), selon lequel le professionnel pouvait appeler tant que la personne ne s'y était pas opposée, disparaît au profit d'un régime de consentement préalable (« opt-in ») : le consentement doit être libre, spécifique, éclairé, univoque et révocable. L'exception principale concerne le contrat en cours, lorsque l'appel a un rapport avec son objet, y compris pour proposer des produits ou services complémentaires.

La CNIL a actualisé ses fiches pratiques sur la prospection commerciale. Elle y intègre le nouveau régime du téléphone à destination des consommateurs et clarifie la frontière entre trois types de communications : commerciale (la promotion, qui exige le consentement), transactionnelle (confirmation de commande, facture, mot de passe) et relationnelle (suivi client, sans visée promotionnelle).

- Obtenir un consentement valable ne suffit toutefois pas : il faut aussi pouvoir prouver qu'il a été obtenu licitement. Le professionnel doit être en mesure de retracer le moment où il a été donné, le canal utilisé, la finalité, la version du formulaire en vigueur à cette date et sa conservation dans le temps. Le défi est donc à la fois probatoire et opérationnel.

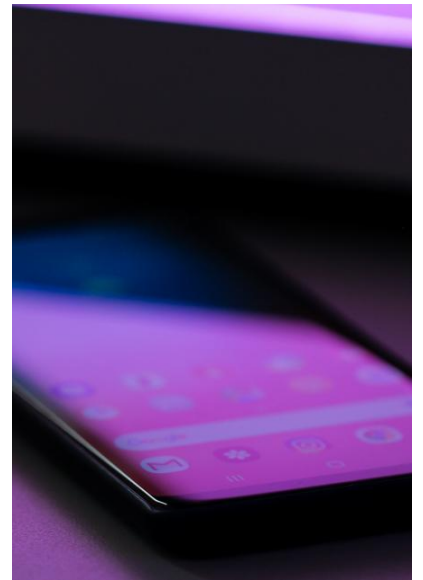
ACTUALITES DONNEES PERSONNELLES

Première notification d'une violation de données imputée à un agent d'intelligence artificielle

L'Agence espagnole de protection des données (AEPD) a reçu la première notification d'une violation de données à caractère personnel imputée à un agent d'intelligence artificielle. Celui-ci serait parvenu à détecter les failles d'une application traitant de telles données, puis à s'y introduire afin d'accéder aux informations et de modifier des factures.

Sans conclure à l'existence d'une tendance statistique, l'AEPD rappelle que l'utilisation malveillante d'outils d'intelligence artificielle est déjà courante, notamment dans le cadre d'opérations d'hameçonnage, et alerte sur l'aggravation de la menace liée au développement de ces outils.

- Selon l'AEPD, cette notification impose de faire évoluer les dispositifs de sécurité existants. Les responsables de traitement doivent désormais intégrer les attaques utilisant l'intelligence artificielle dans leurs analyses de risques, réexaminer leurs délais de réaction, renforcer les mécanismes d'authentification des plateformes et mettre en place des systèmes automatisés de détection.

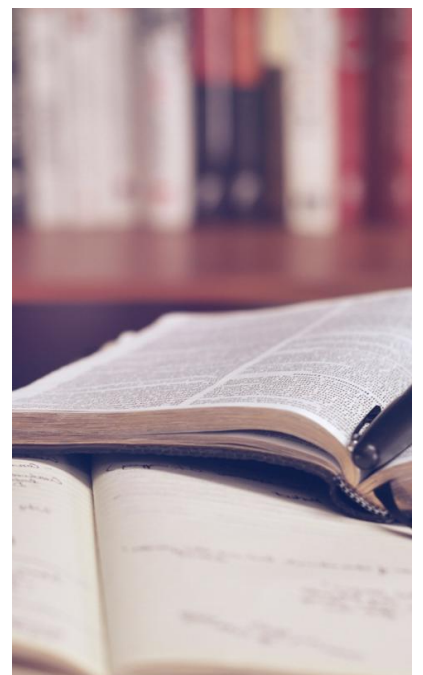


Breaking news AI Act : premières demandes formelles d'informations du Bureau européen de l'IA aux fournisseurs de modèles

Le Bureau européen de l'IA a adressé ses premières demandes formelles d'informations à plusieurs fournisseurs de modèles d'IA à usage général. La vice-présidente exécutive de la Commission, Henna Virkkunen, a présenté cette démarche comme une première étape dans l'application de l'AI Act.

Deux catégories de demandes ont été adressées. La première porte sur la sécurité des modèles, les évaluations externes indépendantes et la surveillance des modèles une fois mis sur le marché. La seconde concerne les résumés du contenu utilisé pour l'entraînement des modèles, et vise les fournisseurs qui n'ont pas publié de détail à ce sujet ni participé aux dialogues informels de conformité menés avec le Bureau de l'IA. Cette seconde catégorie a des implications en matière de droit d'auteur, les titulaires de droits ayant besoin de ces résumés pour déterminer si leurs œuvres ont été utilisées.

Ces demandes sont juridiquement contraignantes : fournir des réponses inexactes, incomplètes ou trompeuses constitue un manquement passible d'une amende. À ce stade, elles ne valent toutefois pas constat de violation de l'AI Act et aucune mesure de restriction n'a été prise à l'encontre d'un modèle.



ACTUALITES DONNEES PERSONNELLES



Uber sanctionné à hauteur de 824,99 millions d'euros pour des décisions automatisées de désactivation de comptes

En août 2026, l'Autorité néerlandaise de protection des données a imposé à Uber une amende de 824,99 millions d'euros. Elle lui reproche d'avoir désactivé des comptes de chauffeurs par des systèmes automatisés, en violation de l'article 22 du RGPD.

La procédure trouve son origine dans une plainte déposée en France en 2020 devant la CNIL par la Ligue des droits de l'homme, qui représentait 171 chauffeurs. Uber ayant son établissement principal aux Pays-Bas, l'autorité néerlandaise était chef de file au titre du guichet unique, la CNIL ayant toutefois été associée à l'instruction. Il s'agit de la troisième sanction prononcée dans ce dossier, après une amende de 10 millions d'euros en 2023 pour manquements à l'information des chauffeurs et une amende de 290 millions d'euros en 2024 pour des transferts de données hors de l'Union européenne.

L'autorité a relevé qu'entre 2018 et 2022, les désactivations de comptes en cas de suspicion de fraude (par exemple des détours pour augmenter le prix de la course) ou de notation basse par les clients avaient été décidées sans aucune intervention humaine. Elle les qualifie de décisions individuelles automatisées au sens de l'article 22 du RGPD, qui affectent les chauffeurs de manière significative puisque la désactivation du compte paralyse leur activité et les prive de revenus. Elle relève en outre que les chauffeurs n'étaient pas suffisamment informés du processus conduisant à la désactivation.

Uber conteste une partie des faits, juge la sanction disproportionnée et a annoncé faire appel. Cette amende serait la deuxième plus lourde prononcée au titre du RGPD, après celle de 1,2 milliard d'euros infligée à Meta en 2023.

- Toute organisation qui exclut, suspend ou note des personnes de manière automatisée doit s'assurer que l'intervention humaine dans le processus de décision est réelle.

ACTUALITES DONNEES PERSONNELLES

Cyberattaque à l'Hôpital privé de la Loire : 500 000 euros d'amende pour des manquements à la sécurité des données de santé

CNIL, formation restreinte, délibération n° SAN-2026-009 du 21 juillet 2026

La CNIL a prononcé une amende de 500 000 euros à l'encontre de l'Hôpital privé de la Loire (HPL), établissement du groupe Ramsay Santé, à la suite d'une cyberattaque d'une ampleur exceptionnelle. Le 1er juillet 2025, l'établissement a découvert l'intrusion d'un attaquant dans son dossier patient informatisé. Celui-ci avait exfiltré 524 867 fiches contenant notamment des données d'état civil et de santé, des numéros de sécurité sociale, des coordonnées et des copies de cartes d'identité, ainsi que les données de 202 246 tiers de confiance. Saisie de la notification et de neuf plaintes, la CNIL a procédé à un contrôle sur place.

Rappelant, à la suite de la Cour de justice de l'Union européenne, que l'article 32 du RGPD institue une obligation de moyens qui peut être méconnue lorsque les mesures de sécurité sont insuffisantes au regard des risques identifiés, la formation restreinte relève cinq défaillances : l'absence d'authentification à deux facteurs pour les accès distants externes, contrairement au référentiel applicable aux services numériques en santé ; un cloisonnement insuffisant des dossiers patients ; l'absence d'analyse automatisée et en temps réel des traces applicatives ; la transmission à tous les praticiens externes d'un même mot de passe temporaire par un tiers ; l'accès permanent et non contrôlé de l'éditeur du logiciel au dossier patient.



Un manquement à l'article 34 du RGPD est également retenu. Si les patients ont été correctement informés, aucune communication directe n'a été adressée aux 202 246 tiers de confiance concernés, la publication d'un communiqué sur le site de l'établissement ne satisfaisant pas à l'exigence d'information individuelle, d'autant que ces personnes n'ont aucune raison de le consulter.

Pour déterminer le plafond et le montant de l'amende, la formation restreinte retient la notion d'« entreprise » au sens des articles 101 et 102 du TFUE et prend ainsi en considération le groupe Ramsay Santé, dont l'hôpital est une filiale. Bien qu'il s'agisse d'une décision d'espèce, sa motivation fournit des enseignements à l'ensemble des établissements de santé utilisant un dossier patient informatisé. La délibération peut faire l'objet d'un recours devant le Conseil d'État dans les deux mois suivant sa notification.

ACTUALITES DONNEES PERSONNELLES

Concurrence déloyale : la détention d'informations confidentielles sur l'ordinateur d'un ancien salarié caractérise leur appropriation par le nouvel employeur

Cour de cassation, chambre commerciale, 2 septembre 2026, pourvoi n° 25-12.718, publié au Bulletin

Par un arrêt du 2 septembre 2026 publié au Bulletin, la Chambre commerciale de la Cour de cassation juge, sur le fondement de l'article 1240 du Code civil, que l'appropriation d'informations confidentielles appartenant à une société concurrente, apportées par un ancien salarié, constitue un acte de concurrence déloyale, même lorsque ce salarié n'est pas tenu par une clause de non-concurrence. Elle ajoute que la seule détention de ces informations sur l'ordinateur professionnel du salarié suffit à caractériser leur appropriation par le nouvel employeur.

En l'espèce, un salarié de la société Fluides service distribution (FSD) avait démissionné avec effet au 28 septembre 2018 pour rejoindre le 1er octobre 2018 une société concurrente, EPAI, son contrat étant transféré en 2019 à une filiale de celle-ci, devenue GSIS. FSD avait fait constater sur l'ordinateur professionnel de l'ancien salarié la présence d'un fichier lui appartenant, comportant les coordonnées de ses clients, ainsi que de plusieurs modèles d'offres de prix, et avait assigné les deux sociétés en 2021.

La cour d'appel de Toulouse avait rejeté les demandes dirigées contre GSIS et limité à 283 euros les dommages et intérêts mis à la charge d'EPAI, au motif que la détention des documents par l'ancien salarié ne prouvait pas leur appropriation par ses nouveaux employeurs, qui contestaient en avoir connaissance. La Cour de cassation censure ce raisonnement : en statuant ainsi, alors que la seule détention de ces informations sur l'ordinateur professionnel caractérise leur appropriation par le nouvel employeur, la cour d'appel n'a pas tiré les conséquences légales de ses constatations. Il en résulte que l'entreprise victime n'a pas à démontrer que le nouvel employeur connaissait l'origine des fichiers ni qu'il les avait effectivement utilisés.

L'arrêt est cassé en ce qu'il rejette la demande de condamnation de GSIS et limite à 283 euros la condamnation d'EPAI. L'affaire est renvoyée devant la cour d'appel de Bordeaux, qui devra réexaminer la responsabilité des sociétés concernées et l'étendue du préjudice économique de FSD.





Stéphanie Berland

Avocate – Associée

T: +33 1 40 69 26 63

E: s.berland@dwf.law



Emmanuel Durand

Avocat – Associé

T: +33 1 40 69 26 83

E: e.durand@dwf.law



Florence Karila

Avocate – Associée

T: +33 1 40 69 26 57

E: f.karila@dwf.law



Anne-Sylvie Vassenaix-Paxton

Avocate – Associée

T: +33 1 40 69 26 51

E: as.vassenaix-paxton@dwf.law

À propos de cette newsletter

Cette newsletter est publiée sous la supervision de **Stéphanie Berland**, Associée.

Le cabinet remercie chaleureusement **Mélissa Boudjella** pour son concours à la préparation de cette publication.

DWF est l'un des principaux fournisseurs mondiaux de services juridiques et commerciaux intégrés.

Notre approche de Gestion Juridique Intégrée offre une plus grande efficacité, une maîtrise des prix et une transparence pour nos clients.

Nous fournissons des services juridiques et commerciaux intégrés à l'échelle mondiale grâce à nos 3 offres, Legal Advisory, Legal Operations et Business Services, dans nos secteurs stratégiques. Nous combinons de manière transparente un certain nombre de nos services pour fournir des solutions sur mesure à nos différents clients.

© DWF, 2026. tous droits réservés. DWF est un nom commercial collectif pour la pratique juridique internationale et l'activité commerciale multidisciplinaire comprenant DWF Group Limited (constitué en Angleterre et au Pays de Galles, immatriculé sous le numéro 11561594, dont le siège social est situé au 20 Fenchurch Street, Londres, EC3M 3AG) et ses filiales et entreprises filiales (telles que définies dans la loi britannique sur les sociétés (Companies Act) de 2006). Pour de plus amples informations sur ces entités et sur la structure du groupe DWF, veuillez vous référer à la page "Mentions légales" de notre site Internet à l'adresse suivante : www.dwfgroup.com. Lorsque nous fournissons des services juridiques, nos avocats sont soumis aux règles de l'organisme de réglementation auprès duquel ils sont admis et les entités du groupe DWF qui fournissent ces services juridiques sont réglementées conformément aux lois pertinentes des juridictions dans lesquelles elles opèrent. Tous les droits sont réservés. Ces informations sont destinées à une discussion générale sur les sujets abordés et ne sont données qu'à titre indicatif. Elles ne constituent pas un avis juridique et ne doivent pas être considérées comme un substitut à un avis juridique. DWF n'est pas responsable de toute activité entreprise sur la base de ces informations et ne fait aucune déclaration ou garantie de quelque nature que ce soit, expresse ou implicite, quant à l'exhaustivité, l'exactitude, la fiabilité ou l'adéquation des informations contenues dans le présent document.

dwfgroup.com