

Newsletter

Tech / Data

2e Trimestre 2026

Google condamné à indemniser M6 à hauteur de 22,69 millions d'euros pour abus de position dominante

Le 10 mars 2026, le tribunal des activités économiques de Paris a sanctionné Google pour ses pratiques en faveur de sa plateforme publicitaire AdX, portant préjudice aux éditeurs, dont M6.

Dans ce numéro

Les fournisseurs de DNS peuvent se voir imposer des mesures de blocage	2
--	---

Amende de 200 millions d'euros infligée à TEMU au titre du DSA	3
--	---

Annulation partielle de la désignation de Meta comme contrôleur d'accès	4
---	---

La non-conformité au RGPD entraine la nullité du contrat pour erreur sur les qualités essentielles du site web	5
--	---

La CJUE encadre strictement la collecte des données biométriques en matière pénale	7
--	---

Décision Conseil d'Etat – transfert de données	8
--	---

La CNIL encadre l'usage des pixels de suivi dans les courriels	9
--	---

Le conseil constitutionnel met fin au cumul des sanctions en matière de prospection électronique	10
--	----

ACTUALITES NOUVELLES TECHNOLOGIES

Les fournisseurs de DNS peuvent se voir imposer des mesures de blocage

Cour d'appel de Paris, 13 mai 2026, n°24/19156

Par un arrêt du 13 mai 2026, la Cour d'appel de Paris confirme la possibilité d'imposer des mesures de blocage à des intermédiaires techniques autres que les fournisseurs d'accès à internet, en particulier les fournisseurs de services de résolution de noms de domaine (DNS), dans le cadre de la lutte contre le piratage sportif.

En l'espèce, le groupe Canal+ sollicitait, sur le fondement de l'article L.333 10 du Code du sport, la mise en œuvre de mesures destinées à empêcher l'accès, depuis la France, à des sites diffusant sans autorisation les matchs de la Ligue des champions 2024/2025. Le Tribunal judiciaire de Paris avait fait droit à ces demandes en enjoignant plusieurs intermédiaires techniques, dont des fournisseurs de DNS, de procéder à des blocages.

Saisie en appel, la Cour confirme tout d'abord la qualité à agir des sociétés du groupe Canal+, en retenant qu'elles justifient de droits exclusifs d'exploitation audiovisuelle ainsi que de droits voisins sur les programmes diffusés.

L'intérêt principal de l'arrêt réside dans la qualification des acteurs visés par les injonctions. En effet, la Cour adopte une conception large de la notion de « personne susceptible de contribuer à remédier à l'atteinte » et juge que les fournisseurs de services DNS constituent des intermédiaires techniques au sens du droit de l'Union. Elle relève que, même si leur rôle est neutre et automatisé, ces services permettent aux utilisateurs d'accéder aux sites litigieux en traduisant les noms de domaine en adresses IP. Ils participent ainsi, indirectement, à la transmission des contenus illicites et peuvent, à ce titre, faire l'objet d'injonctions de blocage. La Cour confirme également l'existence d'atteintes graves et répétées aux droits du titulaire, caractérisées par la diffusion systématique de matchs via des sites de streaming et des services IPTV accessibles depuis la France.

S'agissant des mesures ordonnées, la Cour en valide la proportionnalité. Elle considère que le blocage DNS, bien qu'imparfait et contournable, constitue un moyen efficace pour rendre plus difficile l'accès aux contenus illicites et dissuader les utilisateurs.

Les arguments relatifs à la complexité technique et au coût de ces mesures sont également écartés, la Cour estimant que les opérateurs concernés ne démontrent pas que la mise en œuvre de ces mesures impliquerait des modifications disproportionnées de leur architecture technique.

En outre, la Cour d'appel valide le recours à des injonctions dites dynamiques, permettant d'étendre les mesures de blocage à des sites non encore identifiés, sous le contrôle de l'ARCOM, afin de s'adapter au caractère évolutif des pratiques de piratage.

Enfin, la Cour rejette les demandes de renvoi préjudiciel à la CJUE ainsi que les contestations fondées sur le droit de l'Union, considérant notamment que les mesures en cause ne constituent pas des restrictions générales à la libre prestation de services mais des mesures ciblées et proportionnées.



ACTUALITES NOUVELLES TECHNOLOGIES

Amende de 200 millions d'euros infligée à TEMU au titre du DSA

DSA, la Commission inflige une amende de 200 millions d'euros à Temu, 28 mai 2026

Le 28 mai 2026, la Commission européenne a infligé une amende de 200 millions d'euros à Temu en vertu du [Règlement sur les services numériques \(DSA\)](#) au titre d'un manquement à ses obligations d'évaluation des risques systémiques.

La Commission reproche à Temu de ne pas avoir identifié, analysé et évalué avec diligence les risques liés à la présence de produits illégaux et dangereux sur sa plateforme (jouets pour bébés, chargeurs...), ni le préjudice en résultant pour les consommateurs de l'Union européenne.

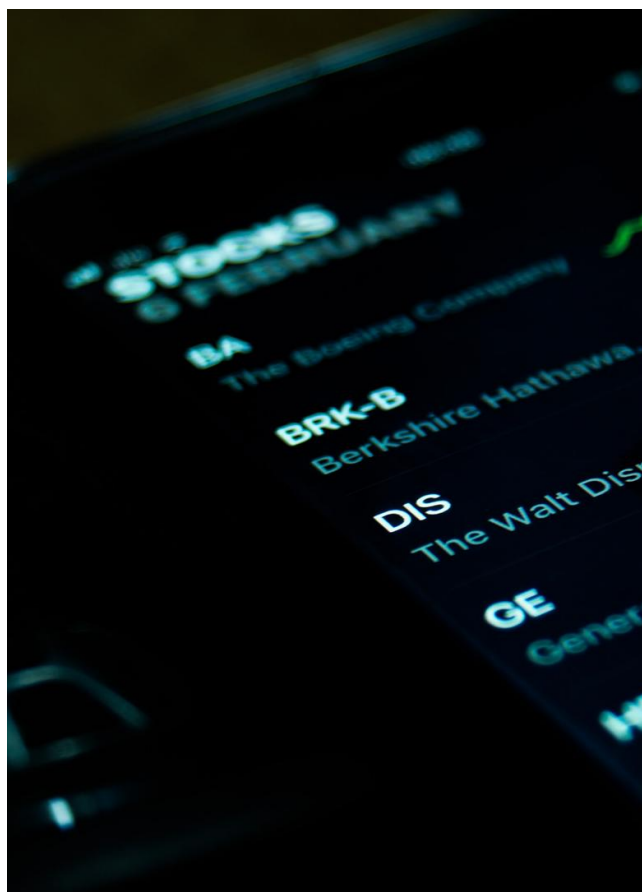
Les éléments de preuve réunis par la Commission, notamment issus des rapports d'évaluation des risques 2024 et intermédiaire 2025 de Temu, de réponses à des demandes formelles de renseignements et d'un exercice de client mystère mené par un organisme d'essai indépendant, démontrent que les consommateurs européens sont très susceptibles de rencontrer des articles illégaux sur la plateforme.

Par ailleurs, l'évaluation des risques réalisée par Temu en 2024 n'était pas conforme aux normes énoncées dans le DSA notamment parce qu'il était basé sur des données générales relatives au secteur du commerce électronique plutôt que sur des preuves spécifiques à son propre service.

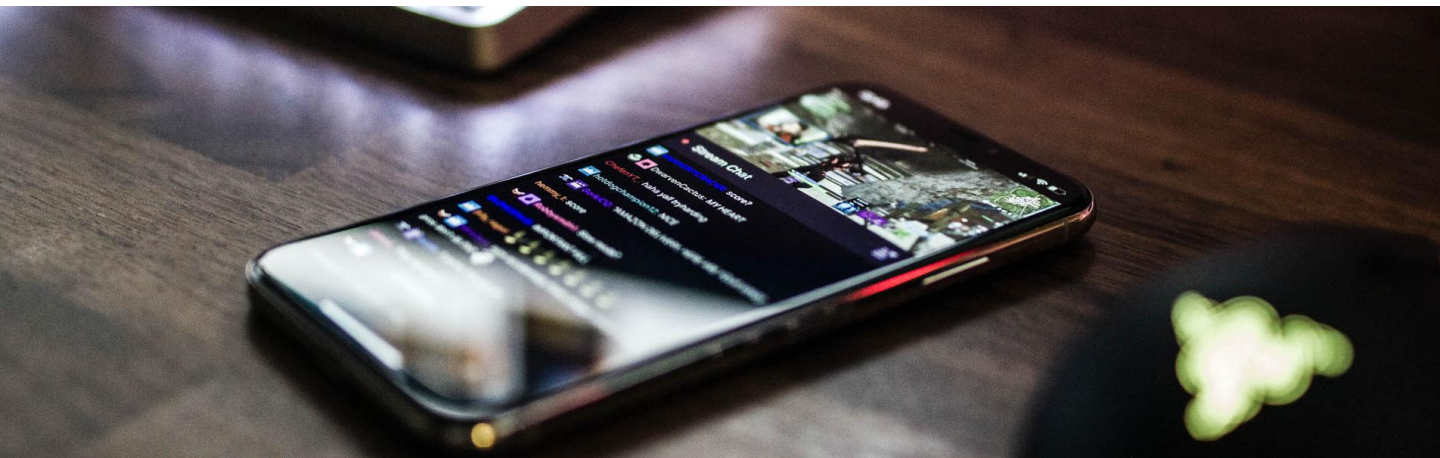
Cette procédure, ouverte le 31 octobre 2024 et ayant fait l'objet de conclusions préliminaires en juillet 2025, se conclut donc par une décision de non-conformité. Le montant de l'amende a été déterminé en tenant compte de la nature de l'infraction, de sa gravité au regard du nombre d'utilisateurs européens concernés et de sa durée, l'absence d'évaluation adéquate des risques constituant, selon la Commission, une violation particulièrement grave de l'une des pierres angulaires du DSA.

Conformément à l'article 75 du règlement, Temu dispose jusqu'au 28 août 2026 pour présenter un plan d'action détaillant les mesures correctrices envisagées. Ce plan sera soumis à l'avis du comité européen des services numériques, qui disposera d'un mois pour se prononcer, avant que la Commission n'adopte sa décision finale dans un délai d'un mois supplémentaire et fixe un calendrier de mise en conformité. Le non-respect de cette décision pourrait donner lieu à des astreintes supplémentaires.

Cette action s'inscrit dans le cadre d'une mobilisation plus large des autorités européennes à l'encontre des grandes plateformes de commerce en ligne à bas prix telles que Shein et AliExpress qui font également l'objet d'enquêtes en raison de manquements potentiels aux règles du DSA, notamment en matière de sécurité des produits, de protection des consommateurs et de gestion des risques systémiques.



ACTUALITES NOUVELLES TECHNOLOGIES



Annulation partielle de la désignation de Meta comme contrôleur d'accès

Tribunal de l'Union européenne, 8ème chambre, Meta Platforms, Inc., c/ Commission européenne, 3 juin 2026, T-1078/23

Par un arrêt du 3 juin 2026, le Tribunal de l'Union européenne a partiellement annulé la [décision de la Commission européenne du 5 septembre 2023](#) désignant Meta comme contrôleur d'accès au titre du [Règlement sur les marchés numériques \(DMA\)](#).

Le Tribunal a ainsi annulé la désignation désignant Meta comme contrôleur d'accès en ce qui concerne Marketplace, tout en confirmant celle de Messenger.

S'agissant de Messenger, le Tribunal confirme qu'il constitue un service de communications interpersonnelles non fondé sur la numérotation distincte du réseau social Facebook. Il souligne que ce service est proposé via des applications autonomes, peut être utilisé indépendamment de Facebook et fait l'objet d'outils spécifiques permettant aux entreprises d'interagir avec les utilisateurs. Les arguments relatifs à l'intégration des services n'ont pas été jugés suffisants pour remettre en cause cette qualification. Le Tribunal valide également l'appréciation de la Commission selon laquelle Messenger constitue, à lui seul, un point d'accès majeur. À ce titre, la Commission n'était pas tenue d'exclure du calcul des utilisateurs finaux ceux qui utilisent également Facebook, ni d'ouvrir une enquête de marché en l'absence d'éléments suffisamment étayés fournis par Meta pour renverser les présomptions prévues par le DMA.

S'agissant de Marketplace, le Tribunal censure en revanche l'analyse de la Commission. Il rappelle que la légalité d'un acte de l'Union doit être appréciée au regard de l'ensemble des éléments de fait et de droit existants à la date de son adoption. Or, la Commission a commis une erreur de droit en limitant son examen aux données des trois années précédentes sans tenir compte des modifications intervenues le 31 juillet 2023. Celles-ci consistaient en une limitation du nombre d'annonces pouvant être publiées par utilisateur et avaient pour effet de faire disparaître le critère utilisé par la Commission pour identifier les entreprises utilisatrices.

En outre, le Tribunal relève une insuffisance de motivation en retenant que la Commission n'a fourni aucune analyse concrète de l'incidence de ces modifications sur la qualification de Marketplace en tant que service d'intermédiation en ligne, se contentant d'éléments hypothétiques et incomplets. Dans ces conditions, la décision ne permettait ni à Meta de comprendre les raisons de cette qualification de service de plateforme essentiel de type service d'intermédiation en ligne, ni au juge de l'Union d'exercer son contrôle.

ACTUALITES DONNEES PERSONNELLES

La non-conformité au RGPD entraîne la nullité du contrat pour erreur sur les qualités essentielles du site web

Cour d'appel de Douai, Chambre 2 section 2, 7 mai 2026, n° 22/05075

Cour d'appel de Lyon, 6e chambre, 5 mars 2026, n° 24/02311

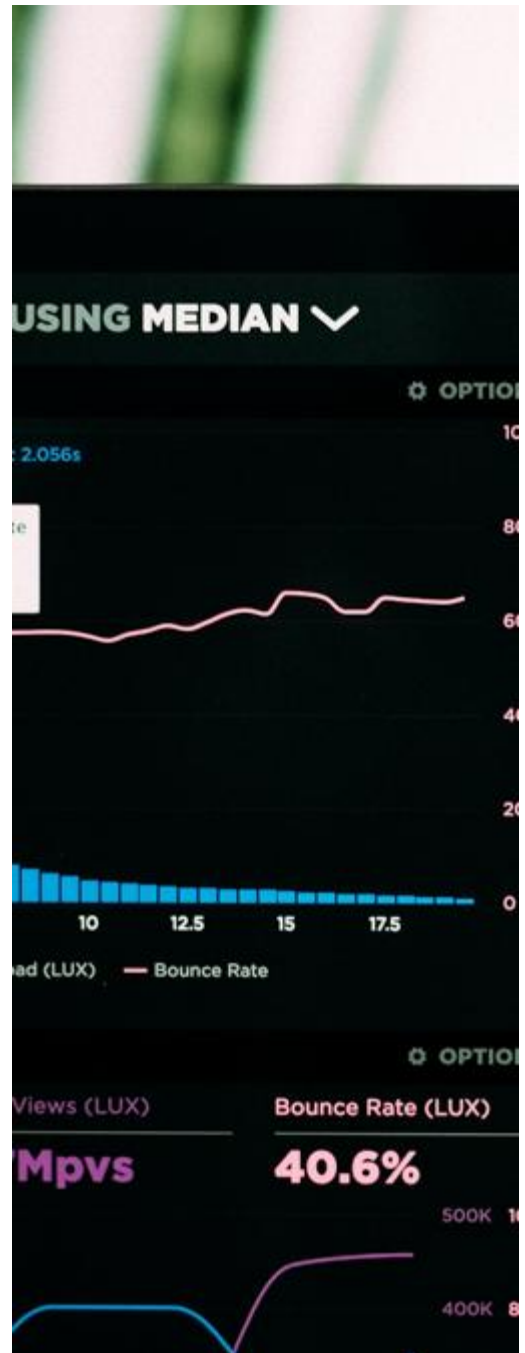
Par un arrêt du 7 mai 2026, la Cour d'appel de Douai a prononcé la nullité d'un contrat de création et de location de site internet en raison de la non-conformité du site livré aux règles impératives relatives à la protection des données personnelles.

En l'espèce, une société avait souscrit auprès d'une agence web un contrat d'abonnement portant sur la création et l'exploitation d'un site internet. Après sa mise en ligne, la société a fait constater par voie d'huissier la présence de cookies déposés sans consentement préalable, ainsi que les dispositifs de collecte de données (formulaire de contact et bouton de rappel) dépourvus de toute information conforme au RGPD.

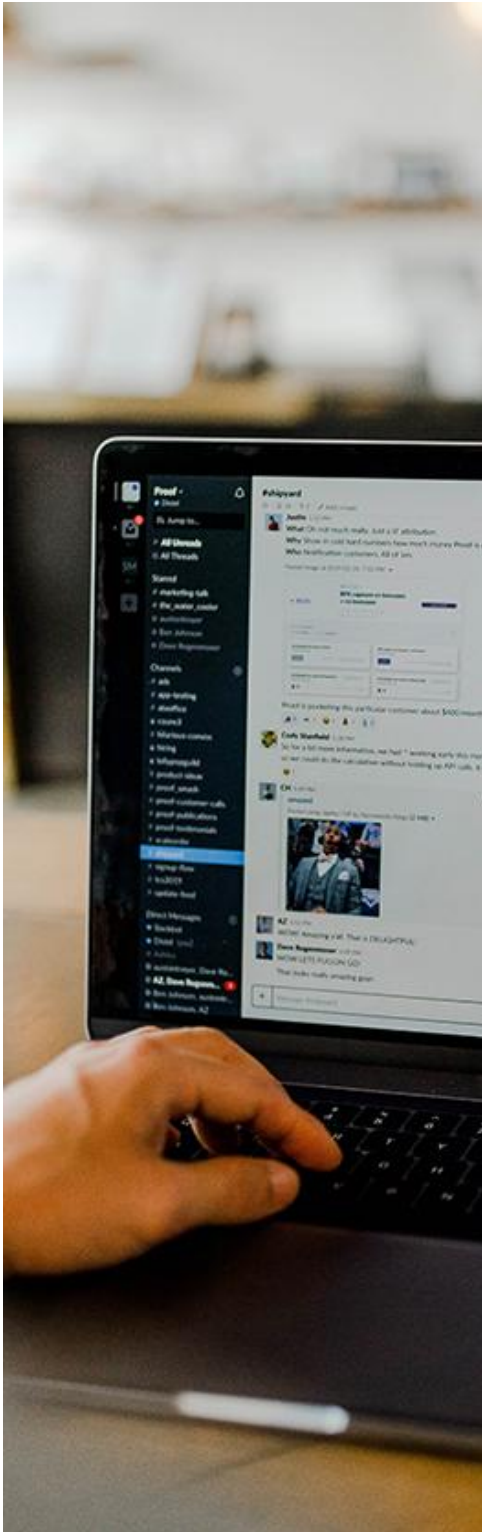
Déboutée en première instance, la société cliente interjette appel en invoquant notamment une erreur sur les qualités essentielles de la prestation tirée de la non-conformité du site à la réglementation sur les données personnelles.

Dans un premier temps, la Cour écarte l'application du droit de la consommation, relevant que la société cliente ne rapporte pas la preuve qu'elle employait cinq salariés au plus lors de la conclusion du contrat, condition exigée pour bénéficier des dispositions protectrices applicables aux professionnels assimilés aux consommateurs.

En revanche, les juges du fond retiennent que la conformité d'un site internet aux règles relatives à la protection des données constitue une qualité essentielle tacitement convenue entre les parties. Ils relèvent plusieurs manquements graves, en particulier l'installation automatique de cookies dès la simple navigation sur le site, sans recueil préalable du consentement des internautes, alors même que certains de ces cookies poursuivaient des finalités publicitaires. Les juges constatent également l'absence de mécanisme effectif permettant de refuser les cookies dès le premier niveau d'information ou de retirer le consentement de manière simple et équivalente à son octroi. À ces manquements s'ajoute également l'absence totale d'information des utilisateurs sur les traitements de données personnelles mis en œuvre via les formulaires de contact et les dispositifs de rappel en violation des exigences du RGPD.



ACTUALITES DONNEES PERSONNELLES



La Cour souligne que le recours à un professionnel spécialisé légitimait l'attente d'un site conforme à la réglementation, d'autant que de tels manquements exposent le client à des risques juridiques et financiers significatifs. Elle en déduit que ces éléments ont vicié le consentement de la société cliente, laquelle n'aurait pas contracté ou l'aurait fait à des conditions différentes si elle avait été informée de ces non-conformités. Le contrat est ainsi annulé pour erreur sur une qualité essentielle de la prestation.

La conformité au RGPD est ainsi reconnue comme une qualité essentielle de la prestation de création de site internet dont la méconnaissance peut vicié le consentement et entraîner la nullité du contrat.

Cette décision s'inscrit dans un mouvement jurisprudentiel déjà affirmé par la Cour d'appel de Lyon le 5 mars 2026. Dans cette affaire, un artisan avait conclu avec la société Linkeo.com un contrat portant sur la création et la mise en ligne d'un site internet, assorti d'un service de maintenance. À la suite d'impayés, le litige a conduit le client à solliciter la nullité du contrat, invoquant notamment la non-conformité du site aux exigences du RGPD.

Confirmant le jugement de première instance, la Cour d'appel de Lyon retient également l'existence d'un vice du consentement résultant de manquements graves aux règles relatives à la protection des données personnelles. Elle relève notamment que des cookies étaient installés sans respect des exigences du RGPD, que leur refus n'empêchait pas leur dépôt, que le retrait du consentement n'était pas aussi simple que son octroi, et que les informations obligatoires relatives au traitement des données faisaient défaut.

La Cour en déduit que le site internet livré ne répondait pas aux attentes légitimes du client, s'agissant d'une qualité essentielle de la prestation fournie par un professionnel. Elle confirme en conséquence la nullité du contrat pour erreur, avec les effets restitutifs qui en découlent.

ACTUALITES DONNEES PERSONNELLES

La CJUE encadre strictement la collecte des données biométriques en matière pénale

CJUE, Comdribus, 19 mars 2026, C-371/24

Par un arrêt du 19 mars 2026, la Cour de justice de l'Union européenne s'est prononcée sur la conformité au droit de l'Union de la législation française autorisant la collecte des empreintes digitales et des photographies de toute personne soupçonnée d'avoir commis ou tenté de commettre une infraction pénale, ainsi que sur la possibilité de sanctionner pénalement le refus de se soumettre à ces opérations de relevés biométriques.

L'affaire concernait un individu interpellé lors d'une manifestation et poursuivi pour avoir refusé de se soumettre à des relevés biométriques alors même qu'il avait été ultérieurement relaxé de l'infraction ayant justifié son interpellation. Condamné uniquement pour le refus de prélèvement, il contestait la conformité de cette condamnation avec la [directive \(UE\) 2016/680 dite « Police Justice »](#).

Saisie à titre préjudiciel par la cour d'appel de Paris, la CJUE rappelle tout d'abord que les empreintes digitales et les photographies constituent des données biométriques relevant des catégories particulières de données à caractère personnel dont le traitement n'est autorisé qu'en cas de « nécessité absolue » au sens de l'article 10 de la directive 2016/680 et que s'il existe des garanties appropriées pour les droits et libertés de la personne concernée.

La Cour affirme que le simple fait qu'il existe une ou plusieurs raisons plausibles de soupçonner qu'une personne a commis ou tenté de commettre une infraction ne suffit pas, à lui seul, à justifier la collecte systématique de ses données biométriques. Une telle collecte n'est conforme au droit de l'Union que si le droit national définit de manière suffisamment précise les finalités poursuivies et impose à l'autorité compétente d'apprécier, dans chaque cas d'espèce, si cette collecte est absolument nécessaire et proportionnée au regard de ces finalités.

En outre, la Cour de justice affirme que l'article 10 de la directive impose à l'autorité compétente une obligation de motivation claire. Celle-ci doit être en mesure d'exposer, pour chaque personne concernée, les raisons pour lesquelles la collecte de données biométriques répond à une nécessité absolue. Cette motivation constitue une garantie essentielle permettant à la personne concernée de comprendre les raisons de cette mesure, de pouvoir exercer son droit à un recours judiciaire effectif et de permettre à la juridiction compétente d'établir un contrôle de la légalité de cette mesure. La Cour souligne également que l'obligation faite à l'autorité compétente de justifier le caractère « strictement nécessaire » de la collecte ne constitue pas une contrainte excessive en ce sens qu'une telle collecte ne saurait, en tout état de cause, être systématique à l'égard des personnes raisonnablement soupçonnées d'avoir commis ou tenté de commettre une infraction pénale pour un ou plusieurs motifs.

Enfin, s'agissant de la sanction pénale du refus de se soumettre aux relevés biométriques, la Cour estime que le droit de l'Union ne s'oppose pas, en principe, à une législation nationale permettant de poursuivre et de condamner une personne pour ce refus, même en l'absence de poursuites ou de condamnation pour l'infraction initiale. Cette possibilité de sanction reste toutefois subordonnée à la double condition que la collecte envisagée soit strictement nécessaire et que la sanction infligée soit proportionnée.



ACTUALITES DONNEES PERSONNELLES

Décision Conseil d'Etat – transfert de données

Conseil d'Etat, Association les licornes célestes et autres et association Interhop, 20 mars 2026, Nos 503159, 504171

Par une décision du 20 mars 2026, le Conseil d'Etat s'est prononcé sur la légalité d'une délibération de la CNIL ayant autorisé l'Agence européenne des médicaments à mettre en œuvre des traitements de données de santé dans le cadre du [projet DARWIN EU](#). Ce projet vise à renforcer la collaboration entre les agences réglementaires et les chercheurs de différents pays européens dans le cadre d'un réseau de partage de données, ressources et expertises.

Plusieurs associations contestaient cette autorisation en raison du recours à la société Microsoft Ireland, filiale de la société Microsoft établie aux Etats-Unis, pour l'hébergement des données issues du système national des données de santé (SNDS). Elles invoquaient notamment le risque de transfert vers les États-Unis et l'insuffisance des garanties techniques et juridiques mises en œuvre.

Par cette décision, le Conseil d'État rejette l'ensemble des recours et valide la position de la CNIL. Il relève en premier lieu que la délibération litigieuse autorise uniquement un traitement de données de santé avec hébergement de ces données dans des centres situés en France et n'a ni pour objet ni pour effet d'autoriser un transfert de données de santé vers les États-Unis. Les requérants ne peuvent donc utilement se prévaloir de l'illégalité de la décision d'adéquation UE/États-Unis ni invoquer une violation de l'interdiction des transferts hors de l'Union européenne.

La Haute juridiction distingue par ailleurs les données de santé des données techniques liées à l'usage de la plateforme. Si ces dernières peuvent faire l'objet de transferts vers les États-Unis, elles ne contiennent aucune donnée sensible et sont encadrées par des clauses contractuelles types constituant des garanties appropriées au sens du RGPD.

S'agissant du respect des exigences du RGPD, le Conseil d'État reconnaît qu'un accès aux données par les autorités américaines ne peut être totalement exclu. Toutefois, il estime que les mesures mises en place telles que la pseudonymisation, la limitation de la durée de conservation, l'analyse des risques de réidentification et la traçabilité des accès, offrent des garanties suffisantes au regard des articles 28 et 32 du RGPD. De plus, le Conseil d'Etat rappelle qu'en dépit pour Microsoft Ireland de bénéficier de la certification « SecNumCloud » délivrée par l'ANSSI, elle dispose toutefois de la certification « hébergeur de données de santé » prévue par le Code de la santé publique (article L. 1111-8 CSP).

Enfin, le juge refuse de saisir la Cour de justice de l'Union européenne, considérant qu'aucune difficulté sérieuse d'interprétation du droit de l'Union ne justifie un renvoi préjudiciel.

Cette décision confirme une approche pragmatique du juge administratif en matière de transferts de données, fondée sur une appréciation concrète des garanties mises en œuvre. Elle admet ainsi le recours à des prestataires liés à des États tiers, y compris les États-Unis, dès lors qu'aucun transfert de données sensibles n'est autorisé et que des mesures de protection appropriées sont effectivement déployées.

ACTUALITES DONNEES PERSONNELLES

La CNIL encadre l'usage des pixels de suivi dans les courriels

CNIL, recommandation relative aux pixels de suivi dans les courriers électroniques, 12 mars 2026



Par une recommandation adoptée le 12 mars 2026, la CNIL encadre l'usage des pixels de suivi dans les courriels, une pratique de plus en plus répandue permettant de mesurer l'ouverture des messages ou de suivre le comportement des destinataires.

Ces pixels, généralement invisibles, reposent sur le chargement à distance d'une image contenant des identifiants permettant de collecter des informations telles que l'ouverture d'un courriel, l'adresse IP ou le terminal utilisé. La CNIL rappelle que leur utilisation constitue une opération de lecture d'informations dans le terminal de l'utilisateur et relève, à ce titre, de l'article 82 de la loi Informatique et Libertés transposant la directive ePrivacy.

La recommandation précise en premier lieu la répartition des rôles entre les différents acteurs impliqués. L'expéditeur du courriel est en principe responsable du traitement, y compris lorsque les pixels sont mis en œuvre par un prestataire d'emailing agissant en qualité de sous-traitant. Lorsque plusieurs acteurs participent à la détermination des finalités, notamment en cas d'exploitation des données à des fins propres, une situation de coresponsabilité peut être retenue.

S'agissant des conditions de licéité, la CNIL affirme que l'utilisation de pixels de suivi nécessite, en principe, le recueil du consentement préalable du destinataire. Ce consentement est notamment requis lorsque les pixels sont utilisés pour analyser les performances des campagnes, personnaliser les communications, établir des profils ou détecter des comportements frauduleux. À l'inverse, certaines finalités peuvent être exemptées de consentement lorsqu'elles sont strictement nécessaires au service demandé. Sont notamment visées les mesures de sécurité contribuant à l'authentification ou certaines opérations limitées à la gestion de la délivrabilité des courriels, à condition qu'elles respectent un principe de minimisation des données et qu'elles concernent des messages sollicités par l'utilisateur, tels que les courriels transactionnels.

La CNIL insiste également sur les modalités de recueil du consentement. Elle recommande de privilégier une collecte de ce consentement au moment de la fourniture de l'adresse électronique afin d'assurer une information claire sur l'utilisation future de traceurs. À défaut, le consentement peut être recueilli ultérieurement via un courriel dépourvu de pixels, renvoyant vers une interface dédiée nécessitant une action positive de l'utilisateur.

Enfin, la recommandation rappelle les exigences classiques du RGPD, notamment la possibilité de retirer son consentement à tout moment, la nécessité d'en conserver la preuve et l'obligation d'assurer une information claire et accessible sur les finalités poursuivies.

ACTUALITES DONNEES PERSONNELLES



Le conseil constitutionnel met fin au cumul des sanctions en matière de prospection électronique

Conseil constitutionnel, décision n° 2026-1210 QPC, Société Orange SA, 25 juin 2026

Saisi d'une question prioritaire de constitutionnalité (QPC) par la société Orange SA, le Conseil constitutionnel s'est prononcé sur la conformité à la Constitution des dispositions de [l'article L.34-5 du Code des postes et des communications électroniques](#) relatives aux sanctions applicables en cas de prospection directe réalisée sans le consentement préalable des personnes concernées.

En l'espèce, ces dispositions permettaient à trois autorités administratives distinctes – la CNIL, l'ARCEP et l'autorité administrative chargée de la concurrence et de la consommation – de sanctionner les mêmes manquements. Les sociétés requérantes soutenaient que ce dispositif méconnaissait le principe constitutionnel de nécessité des délits et des peines en autorisant un cumul de poursuites et de sanctions pour des faits identiques.

Le Conseil constitutionnel accueille cette argumentation. Il relève que les trois autorités sont compétentes pour réprimer les mêmes faits, qualifiés de manière identique, au moyen de sanctions administratives de même nature, poursuivant un objectif commun de protection de la vie privée des utilisateurs contre les sollicitations commerciales non désirées. Un tel dispositif méconnaît le principe de nécessité des délits et des peines garanti par l'article 8 de la Déclaration des droits de l'homme et du citoyen de 1789. Les dispositions contestées sont donc déclarées contraires à la Constitution.

Toutefois, afin d'éviter une remise en cause immédiate de l'ensemble des procédures en cours, le Conseil reporte l'abrogation des dispositions au 31 octobre 2027. Dans l'intervalle, il prévoit qu'aucune nouvelle poursuite ne pourra être engagée par une autre autorité lorsque des poursuites ont déjà été initiées ou lorsqu'une sanction définitive a déjà été prononcée pour les mêmes faits.

Cette décision illustre le rôle central de la QPC dans le contrôle des dispositifs répressifs. Le Conseil constitutionnel rappelle que, même dans des domaines fortement régulés comme la protection des données personnelles et les communications électroniques, le législateur ne peut instaurer plusieurs régimes répressifs conduisant à sanctionner les mêmes faits au nom des mêmes intérêts sociaux. Cette décision conduira nécessairement le législateur à revoir l'articulation des pouvoirs de sanction des différentes autorités administratives indépendantes.



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

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