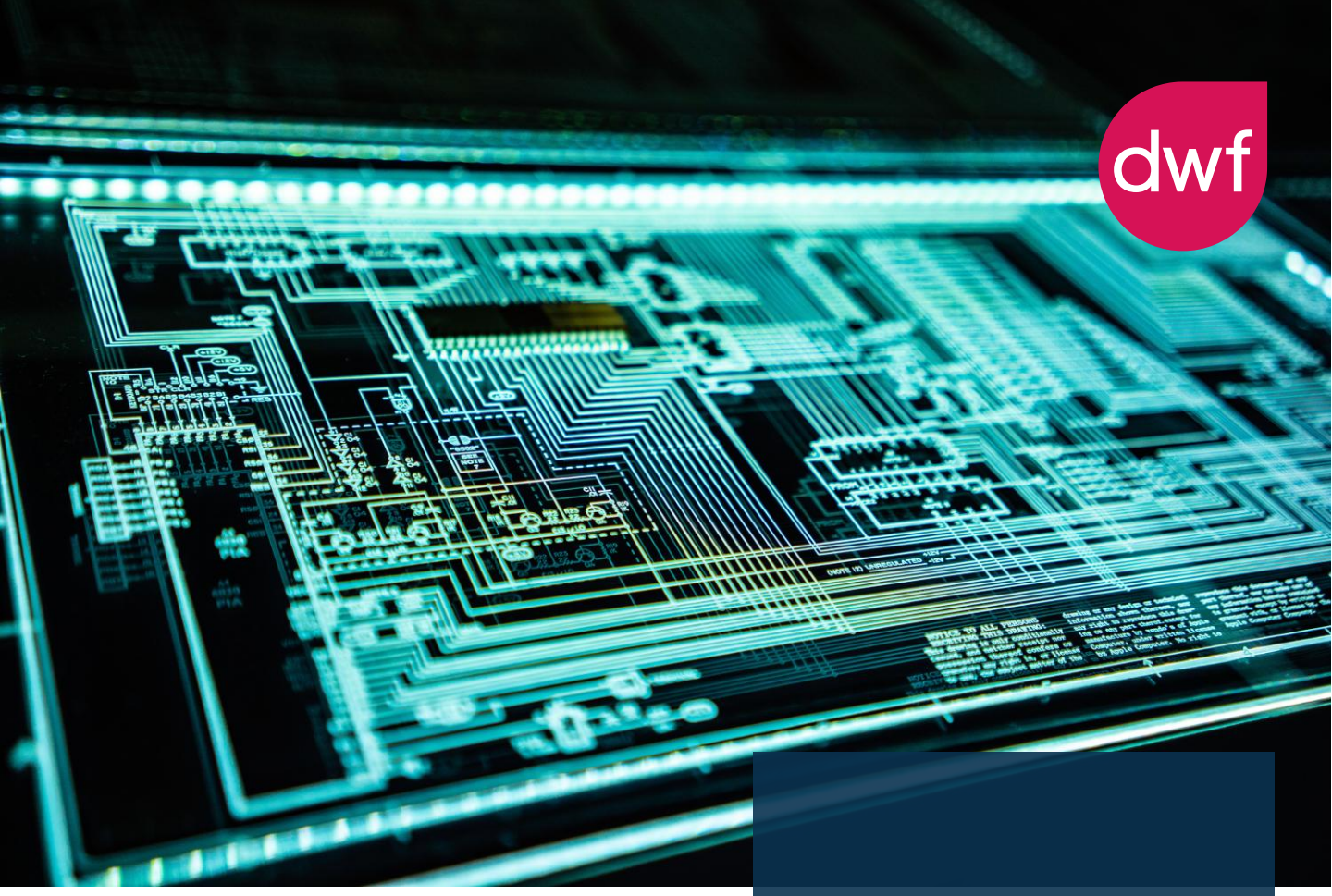


Newsletter

Tech / Data

1er Trimestre 2026

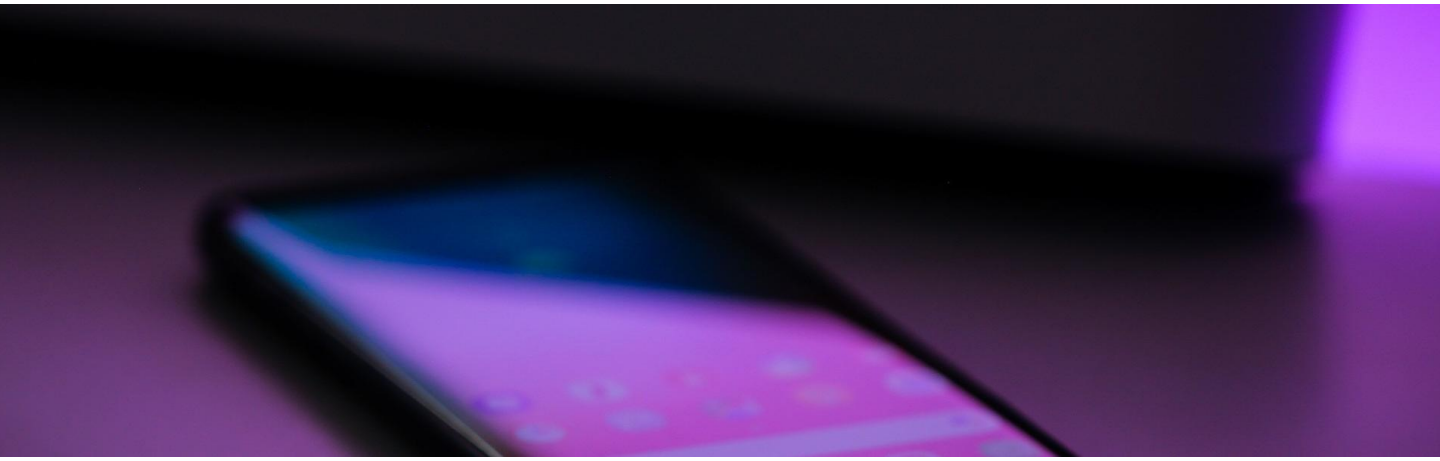
dwfgroup.com

Airbnb privé du statut d'hébergeur

La Cour de cassation juge qu'Airbnb exerce un rôle actif dans la gestion des annonces et ne peut donc bénéficier du régime de responsabilité limité des hébergeurs.

Dans ce numéro

ACTUALITES NOUVELLES TECHNOLOGIES



Condamnation de META pour absence de filtrage des publicités

Cour d'appel de Paris, pôle 5 ch. 1, META PLATEFORMS IRELAND LIMITED c/ GROUPE LUCIEN BARRIERE, 28 janvier 2026, n° 24/12568

Par un arrêt du 28 janvier 2026, la Cour d'appel de Paris confirme les injonctions prononcées à l'encontre de Meta Platforms Ireland Limited après la diffusion répétée, sous forme de publicités sponsorisées, de contenus reproduisant à l'identique la marque du Groupe Lucien Barrière afin de promouvoir des jeux d'argent en ligne illicites.

Estimant ces publicités illicites, le Groupe Lucien Barrière, avait obtenu en urgence une ordonnance imposant à Meta des mesures de filtrage et de conservation des données relatives aux annonceurs concernés. Les obligations mises à la charge de Meta consistaient notamment à mettre en œuvre, sous huit jours, des mesures de prévention ciblant les publicités promouvant des jeux d'argent en ligne reproduisant à l'identique les marques de l'Union européenne « BARRIERE » diffusées par des annonceurs non authentifiés et à assurer pendant douze mois la conservation des données d'identification associées aux comptes concernés.

Meta a formé un recours en rétractation qui a été rejeté par une ordonnance du 24 avril 2024. Dans un arrêt du 28 janvier 2026, la Cour d'appel de Paris considère que les publicités litigieuses portaient atteinte aux fonctions essentielles et économiques des marques de l'Union européenne du Groupe Lucien Barrière et que leur caractère massif, répété et signalé caractérisait un trouble manifestement illicite justifiant l'intervention du juge des référés.

Les juges du fond considèrent que Meta a agi en qualité d'intermédiaire en permettant la publication de publicités dont le caractère est vraisemblablement contrefaisant. De ce fait, ils estiment que Meta peut se voir ordonner des mesures provisoires destinées à faire cesser toute atteinte ou à prévenir une atteinte imminente aux droits de propriété intellectuelle du Groupe Barrière sans que sa responsabilité n'ait à être démontrée ni qu'il soit utile d'établir si Meta a joué un rôle actif dans le déroulement des faits litigieux et si elle doit être considérée comme agissant en qualité d'hébergeur ou d'éditeur au sens de la LCEN et de la directive e-commerce.

La Cour relève en outre que la mesure ordonnée s'est révélée effective pour réduire les contenus litigieux et qu'il n'est pas démontré qu'elle serait disproportionnée au regard des capacités de la société Meta. Elle relève également la conformité de l'injonction dynamique aux orientations européennes en matière de lutte contre les atteintes aux droits de propriété intellectuelle.

La Cour confirme ainsi l'ordonnance du 24 avril 2024 en toutes ses dispositions, rejette la demande formée par Meta au titre de l'article 700 du Code de procédure civile et la condamne à verser au Groupe Lucien Barrière la somme de 15 000 euros à ce titre ainsi qu'aux dépens d'appel.

ACTUALITES NOUVELLES TECHNOLOGIES

Refus d'accorder la qualité d'hébergeur à la plateforme Airbnb

Cour de cassation, chambre commerciale, 7 janvier 2026, n°23-22.723 et n° 24-13.163

Dans deux arrêts du 7 janvier 2026, la Cour de cassation s'est prononcée sur la responsabilité de la plateforme de location en ligne Airbnb dans le cadre d'une sous-location illicite d'un logement social.
Une locataire d'un logement appartenant à la société Famille et Provence avait sous-loué ce bien sur la plateforme Airbnb, en violation de son bail qui lui interdisait toute sous-location. Le bailleur a alors assigné la locataire ainsi que les sociétés exploitant la plateforme afin d'obtenir la restitution des sommes perçues grâce à ces locations.

La Cour d'appel d'Aix-en-Provence avait rejeté la demande dirigée contre la société Airbnb Ireland, considérant que celle-ci n'avait pas la qualité d'éditeur mais celle d'hébergeur, ce qui limitait sa responsabilité.

La Cour de cassation rappelle que le régime de responsabilité allégée prévu pour les hébergeurs par la directive sur le commerce électronique ne s'applique que si le prestataire joue un rôle purement technique et neutre dans le stockage des contenus. En revanche, lorsqu'un opérateur exerce un rôle actif lui conférant une connaissance ou un contrôle des contenus, il ne peut plus bénéficier de ce statut.
Or, selon la Haute juridiction la Cour d'appel n'a pas suffisamment recherché si certaines fonctionnalités de la plateforme, telles que les règles imposées aux utilisateurs, la promotion d'annonces ou l'attribution du statut de « superhost », pouvaient traduire un rôle actif de la société Airbnb dans la gestion des offres publiées.

Ainsi, dans son communiqué la Cour de cassation précise que la société Airbnb n'a pas la qualité d'hébergeur internet car elle ne joue pas un rôle neutre à l'égard des utilisateurs, mais au contraire s'immisce dans la relation entre hôtes et voyageurs en leur imposant de suivre un ensemble de règles et en promouvant certaines offres ayant une influence sur le comportement des utilisateurs.

En ayant ce rôle actif, la société Airbnb ne bénéficie pas de l'exonération de responsabilité que la loi accorde aux hébergeurs.

Avis conjoint du CEPD et de l'EPDS sur la proposition de règlement OMNIBUS

Communiqué sur l'avis du CEPD et de l'EDPS sur une simplification des règles sur l'intelligence artificielle, 13 mars 2026

Le CEPD (Comité Européen de la protection des données) et l'EDPS (Contrôleur européen de la protection des données) ont publié un avis conjoint sur la proposition de règlement Omnibus.

Ceux-ci soutiennent plusieurs avancées comme la simplification des notifications de violations de données, l'harmonisation de la notion de « recherche scientifique », ou encore la nouvelle dérogation pour le traitement de catégories particulières de données aux fins de l'authentification biométrique.

Ils soutiennent également l'objectif consistant à fournir une solution règlementaire pour remédier à la fatigue liée au consentement et à la prolifération des bannières de cookies mais soulèvent dans le même temps les difficultés juridiques et techniques soulevées par la coexistence des deux régimes différents entre les données à caractère personnel et les données à caractère non-personnel.

Ils expriment également des préoccupations majeures notamment concernant la redéfinition des données personnelles jugée trop large et risquant d'affaiblir la protection des personnes ou certaines dérogations liées à l'IA qui nécessitent davantage de garanties et de clarté.

ACTUALITES NOUVELLES TECHNOLOGIES

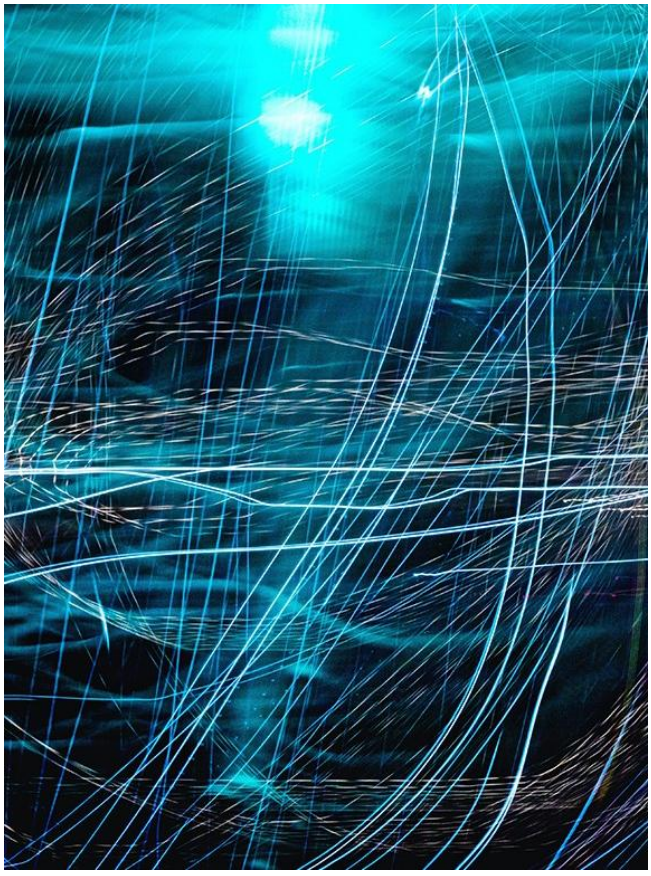
Avis du Conseil de l'Union européenne sur la proposition visant à simplifier et ajuster certaines règles de l'IA Act dans le cadre du paquet de simplification Omnibus

Le Conseil adopte une position visant à simplifier les règles relatives à l'intelligence artificielle, 13 mars 2026

La Commission avait initialement proposé de repousser jusqu'à seize mois l'entrée en application de certaines obligations liées aux systèmes d'IA à haut risque, notamment afin de laisser le temps de produire des standards techniques harmonisés. Elle recommandait également d'étendre les aménagements déjà prévus pour les PME aux small mid-caps, de réduire certaines exigences dans des cas limités, et d'autoriser plus largement l'utilisation de données sensibles aux fins de détection et de mitigation des biais. Elle entendait par ailleurs renforcer les pouvoirs de l'AI Office et réduire la fragmentation du système de gouvernance.

Le Conseil a globalement suivi ces orientations, tout en apportant plusieurs compléments significatifs. Il a notamment introduit une interdiction explicite concernant les pratiques d'IA produisant du contenu sexuel ou intime non consensuel ou du contenu d'abus sexuel d'enfants, renforçant ainsi la protection contre des usages particulièrement préjudiciables. Il a également fixé des dates précises pour l'application différée des règles applicables aux systèmes à haut risque : le **2 décembre 2027** pour les **systèmes autonomes** et le **2 août 2028** pour **ceux intégrés dans des produits**. Par ailleurs, il a rétabli l'obligation pour les fournisseurs d'enregistrer dans la base européenne les systèmes qu'ils estiment exemptés du statut « haut risque », ainsi que la condition de « stricte nécessité » pour le traitement de données sensibles utilisé dans la détection et la correction des biais.

Le texte adopté par le Conseil reporte également au **2 décembre 2027** la date limite pour la mise en place de **bacs à sable réglementaires nationaux**, offrant ainsi plus de marge aux autorités nationales pour organiser ces dispositifs d'expérimentation encadrée. En parallèle, il précise davantage le champ de compétence de l'AI Office quant à la supervision des systèmes basés sur des modèles d'IA d'usage général, en listant notamment les domaines où les autorités nationales conservent un rôle exclusif, tels que l'application de la loi, la gestion des frontières, les autorités judiciaires ou encore certains domaines financiers.



Dans son ensemble, cette position du Conseil vise à accélérer l'application effective du cadre européen sur l'intelligence artificielle tout en garantissant une plus grande proportionnalité des obligations, une meilleure harmonisation entre États membres et un soutien accru aux entreprises. Elle marque un pas important vers une mise en œuvre cohérente et opérationnelle de l'AI Act, dans un contexte où l'UE souhaite renforcer sa compétitivité et instaurer un environnement réglementaire clair tout en protégeant les citoyens contre les usages les plus risqués de l'IA.

ACTUALITES NOUVELLES TECHNOLOGIES

Plateformes de streaming et contenus violents

Tribunal Judiciaire de Paris, Etat français c/ société Kick Streaming, 19 décembre 2025, n°25/57054

Le jugement du Tribunal judiciaire de Paris du 19 décembre 2025 intervient dans un contexte particulier marqué par la diffusion en direct de contenus extrêmement violents sur la plateforme Kick, ayant culminé avec le décès du streamer Jean Pormanove.

Saisi par l'Etat français sur le fondement de la loi pour la confiance dans l'économie numérique (LCEN), le juge devait déterminer dans quelle mesure il pouvait intervenir pour faire cesser ces atteintes tout en respectant la liberté d'expression.

Le Tribunal reconnaît dans un premier temps la compétence du juge judiciaire pour ordonner les mesures visant à prévenir un dommage grave lié à des contenus en ligne. Il admet donc que l'intervention judiciaire est légitime face à la diffusion de contenus violents et accessibles au public français. Cette reconnaissance s'inscrit dans l'articulation entre le droit national (LCEN) et le droit européen, notamment le règlement sur les services numériques (DSA) qui encadre la responsabilité des plateformes.

Cependant, le Tribunal judiciaire refuse de faire droit à la demande principale de l'Etat consistant à bloquer l'ensemble de la plateforme. Il estime qu'une telle mesure serait disproportionnée, faute de preuve d'une dérive systémique de Kick dans son ensemble. Un blocage porterait une atteinte excessive à la liberté d'expression et de communication protégée notamment par la Convention européenne des droits de l'Homme.

En revanche, les juges constatent la gravité particulière des contenus diffusés sur la chaîne « Jean Pormanove », caractérisés par des violences, humiliations et mises en danger. A ce titre, ils ordonnent des mesures ciblées : maintien de l'inaccessibilité de cette chaîne, retrait des contenus violents associés et mise en place d'astreintes financières en cas de non-respect. L'intervention judiciaire est donc admise mais limitée à ce qui est jugé strictement nécessaire. Aucun recours ne semble avoir été formé.

Nouvelle stratégie nationale de cyber sécurité 2026-2030

ANSSI, stratégie nationale de cybersécurité 2026-2030

Le 29 janvier 2026, l'Agence nationale de sécurité des systèmes d'information a publié sa nouvelle stratégie nationale de cybersécurité 2026-2030. Cette stratégie, commandée par le Président de la République, fixe l'ambition de faire de la France une nation cyber de premier rang en réponse à la menace numérique croissante qui touche l'ensemble du tissu économique et social.

Elle place le développement massif des compétences cyber au cœur de l'action publique, avec l'objectif de constituer le plus grand vivier de talents cyber d'Europe, en renforçant toutes les filières de formation et en orientant la jeunesse vers ces métiers d'avenir. Pour consolider la résilience nationale, elle élève le niveau de cybersécurité des infrastructures critiques et des services de l'Etat, améliore la préparation aux crises et renforce l'accompagnement des victimes via un portail national simplifié.

La France entend également freiner l'expansion de la menace en mobilisant tous ses leviers (judiciaires, diplomatiques, militaires, économiques, techniques) et en intensifiant le partage d'informations avec les acteurs privés. La stratégie vise enfin à préserver la souveraineté technologique en investissant dans des technologies critiques (chiffrement, cloud, évaluation de sécurité), en soutenant un marché européen compétitif et en renforçant la coopération internationale pour un cyberespace sûr, ouvert et stable au sein de l'Union Européenne, de l'OTAN et avec ses partenaires.

ACTUALITES DONNEES PERSONNELLES

Demande abusive de droit d'accès au titre du RGPD

CJUE, C-526/24, Brillen Rottler GmbH & Co. KG contre TC, 19 mars 2026

Le 19 mars 2026, la CJUE a précisé qu'une demande d'accès à ses données à caractère personnel peut être qualifiée d'abusive et être refusée si elle est introduite dans le seul but de demander ensuite une réparation pour prétendue violation du RGPD.

Dans cette affaire, un individu résidant en Autriche s'est abonné au bulletin d'information de l'entreprise familiale d'optique Brillen Rottler en renseignant ses données personnelles dans le formulaire d'inscription disponible sur le site Internet de l'entreprise. Treize jours plus tard, il a adressé à Brillen Rottler une demande d'accès au titre du règlement général sur la protection des données (RGPD).

Brillen Rottler a rejeté la demande, estimant qu'elle était abusive. L'entreprise a constaté, à travers divers reportages, articles de blog et bulletins d'avocats, que cet individu s'inscrit systématiquement à des bulletins d'information de différentes entreprises avant d'introduire une demande d'accès, puis une demande de réparation. L'individu, de son côté, considérait que sa demande d'accès était légitime et a demandé à Brillen Rottler une indemnité d'au moins 1 000 euros pour le dommage moral qu'il prétendait avoir subi à la suite du rejet de sa demande.

Le tribunal de district d'Arnsberg, saisi du litige, a interrogé la Cour de justice de l'Union européenne (CJUE) pour savoir si une première demande d'accès aux données personnelles pouvait être considérée comme « excessive » et si la personne concernée avait droit à réparation du dommage résultant d'une violation du droit d'accès.

La CJUE a répondu qu'une première demande d'accès peut, dans certaines circonstances, être considérée comme « excessive » au sens du RGPD et donc être abusive. Cela est le cas lorsque le responsable du traitement démontre que, malgré le respect formel des conditions prévues par le RGPD, la demande a été introduite non pas pour prendre connaissance du traitement des données et vérifier sa légalité, mais avec l'intention abusive de créer artificiellement les conditions nécessaires pour obtenir une réparation en vertu du RGPD. Le fait que la personne ait, selon des informations accessibles au public, introduit plusieurs demandes d'accès suivies de demandes de réparation auprès de différents responsables peut être pris en compte pour établir l'existence d'une telle intention abusive.

Par ailleurs, la Cour a rappelé qu'une personne ayant subi un dommage matériel ou moral du fait d'une violation du RGPD, y compris d'une violation du droit d'accès, a droit à réparation. Cependant, pour obtenir cette réparation, la personne doit démontrer qu'elle a effectivement subi un dommage. Elle ne peut pas obtenir réparation si son propre comportement constitue la cause déterminante du préjudice.

Il revient désormais au tribunal de district d'Arnsberg de trancher le litige en tenant compte de ces précisions apportées par la CJUE.

ACTUALITES DONNEES PERSONNELLES

Le Conseil d'Etat se prononce sur la vidéosurveillance algorithmique

Conseil d'Etat, Commune de Nice c/ CNIL, 30 janvier 2026, n°506370

A la suite d'un contrôle effectué en 2023, la CNIL avait mis en demeure la commune de Nice de produire une analyse d'impact relative à la protection des données concernant plusieurs traitements algorithmiques appliqués aux images de vidéo protection.

Dans son avis du 15 mai 2025, la CNIL a estimé que le dispositif « zone d'intrusion entrée des écoles », destiné à détecter automatiquement et en temps réel les véhicules stationnés irrégulièrement devant les établissements scolaires afin d'alerter la police municipale ne pouvaient être mis en œuvre en l'état du droit applicable.

Le Conseil d'Etat a été saisi par la commune de Nice d'un recours en annulation pour excès de pouvoir contre cette délibération de la CNIL du 15 mai 2025. La commune sollicitait également la condamnation de la CNIL au titre des frais de justice.

S'agissant de la légalité externe, le Conseil d'Etat a jugé que la délibération avait été adoptée dans des conditions régulières tant au regard des règles de quorum que des exigences de motivation. Les moyens tirés d'un vice de procédure et d'une insuffisance de motivation ont donc été écartés.
Sur le fond, le Conseil d'Etat a considéré que si le Code de la sécurité intérieure autorise la mise en œuvre des systèmes de vidéo protection sur la voie publique, ces dispositions ne permettent pas, en l'absence de texte spécifique, l'analyse algorithmique systématique et automatisée des images collectées. Aucune autre base légale ne venant autoriser un tel traitement, la CNIL n'a ni commis d'erreur de droit ni excédé sa compétence en estimant que le dispositif ne pouvait être déployé dans le cadre législatif actuel.

La requête de la commune de Nice ainsi que ses conclusions relatives aux frais de justice sont donc rejetées.

Mise en œuvre de la pseudonymisation

Conseil d'Etat, société GERS c/ CNIL, 13 février 2026, n° 498628

Dans une décision du 13 février 2026, le Conseil d'Etat rappelle que le traitement de données de santé pseudonymisées demeurent soumis au RGPD dès lors que le risque de réidentification n'est pas nul.

Une société contestait deux décisions de la formation restreinte de la CNIL prises le 28 août 2024, lui infligeant des amendes respectives de 800.000 et 200.000 euros. Ces sanctions visaient des traitements de données réalisés à partir de bases issues notamment de cabinets médicaux et d'officines, dans lesquelles les données de santé étaient seulement pseudonymisées. La société soutenait en revanche que ces données étaient anonymisées et ne relevaient donc pas du RGPD, et sollicitait à titre subsidiaire une réformation de la sanction ou une question préjudicielle à la CJUE.

Saisi, le Conseil d'Etat devait déterminer si les données traitées étaient réellement anonymes, ce qui les exclurait du champ du RGPD, ou si le risque de réidentification demeurait. La juridiction rappelle que la pseudonymisation, aussi poussée soit-elle, ne constitue pas une anonymisation lorsque le risque de retrouver l'identité d'une personne n'est pas insignifiant. L'évaluation doit être concrète, fondée sur l'ensemble des données et sources disponibles, et non sur les seules mesures annoncées par le responsable de traitement.

En l'espèce, le Conseil d'Etat confirme que les bases exploitées contenaient des données de santé pseudonymisées, issues de logiciels médicaux ou pharmaceutiques, et que celles-ci restaient réidentifiables compte tenu du croisement possible avec d'autres informations. Dès lors, la juridiction affirme que les traitements relevaient bien du RGPD et nécessitaient un fondement légal conforme, ce qui faisait défaut. Les arguments de la société sur la prétendue anonymisation des données ou sur l'absence de risque raisonnable de réidentification sont donc rejetés.

Plusieurs manquements sont donc constatés, notamment en matière de licéité du traitement, de protection des données de santé et d'absence de consentement adapté, confirmant ainsi les sanctions de la CNIL. Le Conseil d'Etat refuse également de transmettre la question préjudicielle à la CJUE estimant que le cadre juridique applicable est clair.

ACTUALITES DONNEES PERSONNELLES

Accès au dossier du salarié dans le cadre d'une enquête interne

Cour de cassation, Chambre sociale, société Saleforce.com c/ M.[D][I],14 janvier 2026, 24-13.234

Dans un arrêt du 14 janvier 2026, la Cour de cassation rappelle les contours du droit d'accès au dossier dans le cadre d'une enquête interne préalable à un licenciement. Saisis par un ancien salarié d'une société, les juges devaient déterminer si l'absence d'accès complet à l'enquête rendait le licenciement irrégulier.

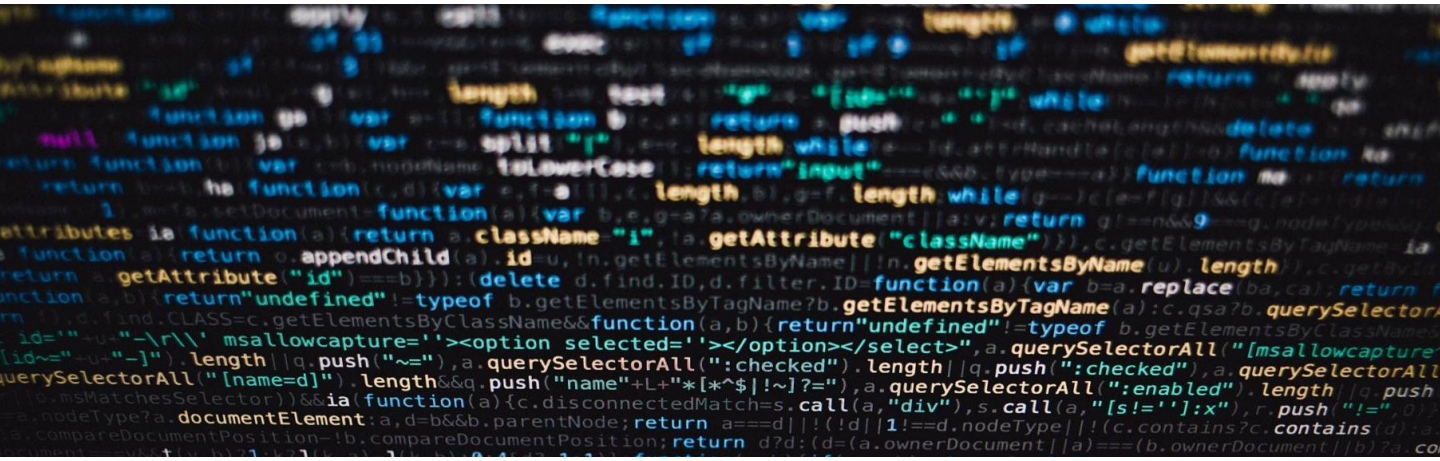
Un vice-président régional, licencié pour faute grave à l'issue d'une enquête interne déclenchée dans le cadre d'un dispositif d'alerte, contestait la validité de la rupture. Il soutenait notamment que l'employeur avait méconnu le code de conduite de l'entreprise en ne lui communiquant pas de manière détaillée les faits dénoncés, ni l'identité des personnes concernées, et en ne lui donnant pas accès au rapport d'enquête, rendant ainsi son licenciement illicite.

La Cour rejette cette argumentation en rappelant que le code de conduite encadrant la procédure d'alerte ne crée pas une procédure disciplinaire autonome. Il organise seulement un traitement d'alerte mais n'impose pas la communication exhaustive et détaillée de l'ensemble des faits dénoncés, ni l'identité des éventuelles victimes.

La Haute juridiction affirme que dans le cadre d'une enquête interne destinée à vérifier des faits signalés, le respect des droits de la défense et du principe du contradictoire n'implique pas un droit d'accès intégral au dossier d'enquête, la communication de toutes les pièces recueillies, ni la confrontation avec les employés ayant mis en cause le salarié.

Il suffit que le salarié soit informé de l'existence de l'enquête, de la nature des faits reprochés et qu'il ait la possibilité de s'expliquer avant la décision de licenciement.

ACTUALITES DONNEES PERSONNELLES



La CNIL sanctionne France TRAVAIL pour absence de sécurité des données

CNIL, France Travail, délibération SAN–2026-003, 22 janvier 2026

À la suite d'une intrusion en 2024, des attaquants ont pénétré dans le système d'information de France Travail en utilisant des techniques d'ingénierie sociale consistant à exploiter la confiance, l'ignorance ou la crédulité des personnes. Cela leur a permis de s'emparer des comptes des conseillers de CAP EMPLOI, une organisation spécialisée dans l'emploi des personnes handicapées.

Cette attaque leur a donné accès aux données de toutes les personnes qui s'étaient inscrites au cours des 20 dernières années, en plus de celles qui avaient un compte candidat sur France Travail, y compris les numéros de sécurité sociale, les adresses électroniques et postales, et les numéros de téléphone. L'attaque ne leur a pas permis d'accéder à des fichiers complets pouvant contenir des données sensibles telles que des données de santé.

L'enquête de la CNIL a révélé de graves lacunes dans les mesures techniques et organisationnelles mises en œuvre par France Travail pour assurer la sécurité des données à caractère personnel traitées, qui auraient pu rendre la violation plus difficile.

La CNIL a identifié les violations suivantes :

- Les méthodes d'authentification permettant aux conseillers CAP EMPLOI d'accéder au système d'information France Travail n'étaient pas suffisamment robustes.
- Il n'existait pas de mesures de journalisation permettant de détecter les comportements inhabituels sur le système d'information.
- Les autorisations d'accès aux comptes des conseillers CAP EMPLOI avaient été définies de manière trop large, permettant aux conseillers CAP EMPLOI d'accéder aux données de personnes qu'ils ne suivaient pas, ce qui a augmenté le volume de données accessibles aux pirates informatiques.

Ces manquements constituent une violation de l'article 32 du RGPD, qui impose au responsable du traitement et au sous-traitant de garantir la sécurité des données à caractère personnel en mettant en œuvre des mesures de sécurité adaptées aux risques.

La formation restreinte de la CNIL a infligé à France Travail une amende de 5 millions d'euros et a ordonné à l'organisation de mettre en œuvre des mesures correctives selon un calendrier précis, sous peine d'une astreinte de 5 000 euros par jour de retard. La sanction tient compte du fait que la plupart des analyses d'impact réalisées par France Travail avant la mise en œuvre du traitement des données avaient déjà identifié des mesures de sécurité adéquates, mais celles-ci n'avaient pas été mises en œuvre.

ACTUALITES DONNEES PERSONNELLES

La CNIL sanctionne une entreprise pour transfert de données à des fins de publicité ciblée

CNIL, anonyme, délibération SAN-2025-017, 30 décembre 2025

En janvier 2023, la CNIL a mené plusieurs enquêtes sur une entreprise, au cours desquelles elle a découvert que celle-ci transmettait depuis plusieurs années les adresses électroniques et/ou les numéros de téléphone des membres de son programme de fidélité à un réseau social à des fins de publicité ciblée.

À l'issue de ces enquêtes, la CNIL a constaté plusieurs manquements aux exigences du RGPD et de la loi française sur la protection des données :

- Le consentement des personnes concernées n'avait pas été obtenu de manière licite, aucune information n'ayant été fournie ou clairement indiquée dans le formulaire d'adhésion et les documents accessibles concernant le transfert de données à des fins publicitaires. Le consentement donné par les personnes concernées n'était ni explicite, ni éclairé, ce qui constitue un manquement à l'obligation d'avoir une base légale conformément à l'article 6 du RGPD.
- Les finalités du traitement des données ont été fournies de manière inexacte et incomplète, ce qui constitue une violation des articles 12 et 13 du RGPD relatifs à l'obligation d'informer les personnes concernées.
- Les règles relatives à la complexité des mots de passe des comptes utilisateurs n'étaient pas suffisamment robustes, ce qui constitue une violation de l'obligation d'assurer la sécurité des données (article 32 du RGPD).
- L'entreprise n'avait pas réalisé d'analyse d'impact, alors que le traitement de la publicité ciblée comportait un risque élevé pour les droits et libertés des personnes concernées, ce qui constitue une violation de l'article 35 du RGPD.
- La CNIL a constaté que onze cookies soumis à consentement étaient placés sur les appareils des utilisateurs dès leur visite sur le site web, n'étaient pas supprimés et continuaient d'être lus même après le refus du consentement, en violation de l'article 82 de la loi française sur la protection des données.

La CNIL et ses 16 homologues européens ont infligé une amende de 3,5 millions d'euros à l'entreprise et ont décidé de publier leurs délibérations afin de rappeler les règles applicables à la publicité ciblée sur les réseaux sociaux. Le montant de l'amende tient compte du nombre élevé de personnes concernées (plus de 10,5 millions) et de la généralisation de ces pratiques.

ACTUALITES DONNEES PERSONNELLES

Sanctions de la CNIL à l'encontre des sociétés FREE et FREE MOBILE

CNIL, FREE et FREE MOBILE, délibération SAN-2026-001, 8 janvier 2026

Le 13 janvier 2026, la CNIL a rendu deux décisions de sanctions à l'encontre des sociétés FREE et FREE MOBILE, prononçant respectivement des amendes de 27 et 15 millions d'euros, compte tenu du caractère inadapté des mesures prises pour assurer la sécurité des données de leurs abonnés.

En octobre 2024, un attaquant a réussi à pénétrer dans le système informatique des entreprises et à accéder aux données personnelles liées à 24 millions de contrats d'abonnés. Certaines informations sensibles ont été compromises, notamment des IBAN pour les clients ayant des services auprès des deux sociétés. Cette fuite a entraîné plus de 2 500 plaintes de personnes concernées, ce qui a conduit la CNIL à ouvrir une enquête.

À l'issue du contrôle, la CNIL a constaté plusieurs manquements au RGPD :

- Les mesures de sécurité mises en place pour protéger les données étaient jugées insuffisantes : par exemple, l'authentification pour accéder au VPN interne n'était pas assez robuste et les mécanismes de détection d'activités suspectes étaient inefficaces. Ces faiblesses ont facilité l'attaque et démontré que la protection des données n'était pas adaptée à la sensibilité et au volume des informations traitées.
- La CNIL a également reproché aux sociétés d'avoir mal informé les personnes concernées par la violation de données : l'email envoyé ne contenait pas toutes les informations exigées par le RGPD pour comprendre les risques et les mesures de protection possibles. De plus, la société FREE MOBILE conservait des données d'anciens abonnés pendant une durée excessive, sans mécanisme suffisant de tri ou de suppression.

En conséquence, la CNIL a infligé 27 millions d'euros d'amende à FREE MOBILE et 15 millions d'euros à FREE, soit 42 millions d'euros au total. Les entreprises ont aussi reçu l'ordre de renforcer rapidement leurs mesures de sécurité et d'améliorer la gestion et la suppression des données personnelles.

ACTUALITES DONNEES PERSONNELLES

La CNIL publie ses recommandations finales sur le consentement multi-terminaux

Recommandation proposant des modalités pratiques de mise en conformité du consentement multi-terminaux, 18 décembre 2025

La CNIL a publié ses recommandations finales sur le consentement multi terminaux pour l'utilisation des cookies et autres traceurs, afin d'aider les responsables de traitement à se conformer au RGPD et à la loi « Informatique et Libertés ». Ces recommandations concernent les environnements web et applications mobiles, mais peuvent aussi guider d'autres contextes nécessitant un consentement, comme les télévisions connectées, consoles de jeux, assistants vocaux, objets connectés ou véhicules connectés. Elles s'appliquent aux utilisateurs authentifiés à un compte ainsi qu'aux utilisateurs non authentifiés, même si le consentement multi terminaux ne s'applique lui qu'aux utilisateurs connectés.

Le consentement multi terminaux permet à un utilisateur de définir ses choix concernant les cookies et traceurs sur un appareil, et de les appliquer automatiquement sur tous ses autres terminaux connectés au même compte. Ce mécanisme est facultatif, mais il doit respecter les principes de consentement libre, éclairé, spécifique et univoque. L'utilisateur doit être informé de la portée de ses choix avant de les exprimer, et il doit pouvoir gérer ses préférences sur chaque terminal, via un panneau de contrôle ou un centre de préférences.

La CNIL recommande également de prévoir des modalités claires pour gérer les contradictions entre les choix formulés sur un terminal non authentifié et ceux enregistrés sur le compte.

Deux approches sont possibles : soit les derniers choix effectués sur un terminal écrasent ceux du compte, soit ce sont les choix du compte qui prévalent. Dans tous les cas, l'utilisateur doit être informé de la situation et des moyens pour modifier ses choix.

Par ailleurs, les responsables de traitement doivent minimiser les données personnelles transmises à des prestataires externes impliqués dans la gestion du consentement, par exemple en utilisant un identifiant technique plutôt que l'identifiant du compte contenant des informations personnelles. Enfin, lors de la mise en place d'un mécanisme multi-terminaux, il est nécessaire de recueillir un nouveau consentement afin que l'utilisateur soit informé de la portée multi-terminaux de ses choix.

INFOS RAPIDES

La Commission européenne a adopté le 27 janvier 2026 une décision d'adéquation reconnaissant que le Brésil garantit un niveau de protection des données personnelles « essentiellement équivalent » à celui de l'Union européenne, ce qui permets aux données personnelles de circuler entre l'UE et le Brésil sans formalités supplémentaires.

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 huit secteurs clés. Nous combinons de manière transparente un certain nombre de nos services pour fournir des solutions sur mesure à nos différents clients.

dwfgroup.com