NEWSLETTER

TECH / DATA

STEERING LEGAL

DANS CE NUMÉRO

Adoption du règlement sur l'IA

Le 2 février 2024, les 27 pays membres de l'Union européenne ont voté à l'unanimité en faveur de l'AI Act, un texte législatif crucial qui établit des principes fondamentaux pour réguler l'utilisation de l'intelligence artificielle (IA) en fonction des risques identifiés. Découvrez dans notre article les apports de ce texte.

ACTUALITÉS NOUVELLES TECHNOLOGIES

Adoption du règlement sur l'IA

Règlement UE concernant l'intelligence artificielle, COM/2021/206 final

Le 2 février 2024, les 27 pays de l'UE ont adopté à l'unanimité l'AI Act. Ce texte vise à encadrer l'utilisation de l'IA et prévoir des obligations à la charge tant des fournisseurs et distributeurs de systèmes d'IA que des utilisateurs. Il s'appliquera à toutes les organisations et entreprises quelle que soit leur taille et les entités publiques établies dans l'UE mais aussi à celles qui commercialisent leurs systèmes et modèles dans l'UE. Ces obligations dépendent du niveau de risque identifié :

- **Risque inacceptable** : ces systèmes et modèles d'IA sont interdits et ne peuvent être ni mis sur le marché dans l'UE, ni exportés. Il s'agit notamment des systèmes de catégorisation biométrique utilisant des caractéristiques sensibles (opinions politiques, religieuses, etc.) et de ceux procédant à l'extraction non ciblée d'images faciales pour la constitution de base de données de reconnaissance faciale, des systèmes de reconnaissance des émotions, de notation sociale. Le délai pour se mettre en conformité est de 6 mois après la publication de l'IA Act, soit vers novembre 2024. La sanction en cas de violation peut aller jusqu'à 35 millions d'euros ou 7% du chiffre d'affaires annuel mondial ;
- **Haut risque** : il s'agit des systèmes déployés pour les produits et domaines d'activité définis aux annexes II et III* de l'IA Act. Ils devront faire l'objet d'une déclaration de conformité et d'un enregistrement dans la base de données de l'UE et obtenir un marquage CE lorsque le cas d'usage est à haut risque. Ces obligations sont applicables 24 ou 36 mois après la publication de l'IA Act en fonction du cas d'espèce. La sanction ira jusqu'à 15 millions d'euros ou 3% du chiffre d'affaires annuel mondial ;
- **Risque faible** : ces systèmes et modèles d'IA sont ceux qui interagissent avec des personnes physiques. Ils doivent respecter des obligations d'information et de transparence envers les utilisateurs, ces obligations étant applicables 24 mois après la publication de l'IA Act. Le plafond de la sanction est de 7.5 millions d'euros ou 1% du chiffre d'affaires annuel mondial ;
- **Risque minime** : ces systèmes et modèles d'IA peuvent suivre volontairement des codes de conduite. Le délai de mise en œuvre est de 24 mois après la publication de l'IA Act, soit vers octobre 2026.

Par ailleurs, les IA à usage général comme ChatGPT, devront fournir un résumé suffisamment détaillé sur les données utilisées conformément aux nouvelles obligations de transparence, et respecter la règlementation relative au droit d'auteur. Des procédures d'opt-out devraient donc être mises en place afin que les ayants-droit puissent s'opposer à la fouille et l'analyse automatisée des données.

Une cartographie des systèmes d'IA détenus par l'entité devra être effectuée, ainsi qu'une analyse des risques afin de classer les systèmes ou modèles existants selon les différents niveaux précités, les obligations prévues par l'IA Act s'appliquant à chaque système ou modèle d'IA individuellement et non à l'organisation dans son ensemble.

Les dates précisées ci-dessus sont à confirmer, la ratification de l'IA Act étant prévu pour le mois d'avril 2024, il entrera en vigueur à la date définie dans l'acte ou, à défaut, 20 jours après sa publication au Journal officiel de l'Union européenne.

**Identification biométrique, infrastructures critiques, éducation, emploi, services privés essentiels, forces de l'ordre, migration, justice*

ACTUALITÉS NOUVELLES TECHNOLOGIES

Adoption du premier schéma de certification européen (EUCC)

Schéma de certification européen (EUCC), 31 janvier 2024

Le 31 janvier 2024, la Commission Européenne a adopté le premier schéma de certification européen, EUCC (EU Common Criteria), conforme au règlement de l'UE sur la cybersécurité. Ce schéma de certification propose un ensemble de règles et de procédures à l'échelle de l'Union sur la manière de certifier les produits TIC (technologie de l'information et des communications) tout au long de leur cycle de vie et de les rendre ainsi plus fiables pour les utilisateurs. Il sera publié prochainement au Journal officiel de l'UE et entrera en vigueur 20 jours après sa publication. Les premiers certificats pourront être délivrés un an plus tard.

Consultation publique de l'autorité de la concurrence sur l'IA générative

L'autorité de la concurrence (ADLC) s'est autosaisie et a lancé une consultation publique afin d'analyser le fonctionnement concurrentiel du secteur de l'IA générative. L'ADLC indique s'intéresser particulièrement aux pratiques mises en œuvre par les acteurs déjà présents sur l'infrastructure cloud et aux problématiques liées à l'accès à ces infrastructures, aux données et à une main d'œuvre qualifiée. Les acteurs sont invités à répondre aux questions formulées par l'Autorité et à adresser leurs réponses avant le **22 mars 2024**.

EUCS : l'appel des industriels du cloud français pour la création d'une certification exigeante

Les industriels français du cloud ont demandé à l'État et aux décideurs européens de soutenir pleinement le projet de certification européenne pour le cloud. En effet, si la France a adopté la certification la plus rigoureuse, le SecNum Cloud, les autres États membres ont leurs propres systèmes de certification qui présentent des niveaux d'exigence inégaux. Cela fait plusieurs années déjà que l'Union européenne discute du projet de certification EUCS (European Cybersecurity Certification Scheme for Cloud Services) visant à harmoniser les normes de cybersécurité entre les États membres.

Si les débats concernant l'EUCS semblaient converger vers une certification à plusieurs niveaux, incluant des critères exigeants tels que la localisation européenne des fournisseurs de cloud, cette exigence est actuellement remise en cause.

Ainsi, les industriels français souhaitent que soit créé une certification EUCS plus stricte et protectrice et indiquent que l'abandon des exigences concernant la localisation des données dans les niveaux les plus élevés de la certification, risque de faire perdre l'Europe en autonomie, et de renforcer sa dépendance technologique et économique vis-à-vis des GAFAM.

Création d'un Bureau européen de l'intelligence artificielle

Comm. UE, déc., 24 janvier 2024, créant le Bureau européen de l'intelligence artificielle : JOUE 14 févr. 2024, C/2024/1459

La Commission européenne, par une décision du 24 janvier 2024 a créé le Bureau européen de l'intelligence artificielle. Ce bureau à vocation mondiale a pour mission de surveiller l'évolution des modèles d'intelligence artificielle, en particulier ceux à usage général, ainsi que l'interaction avec la communauté scientifique. Il fait partie de la structure administrative de la direction générale des réseaux de communication, du contenu et des technologies.

ACTUALITÉS NOUVELLES TECHNOLOGIES

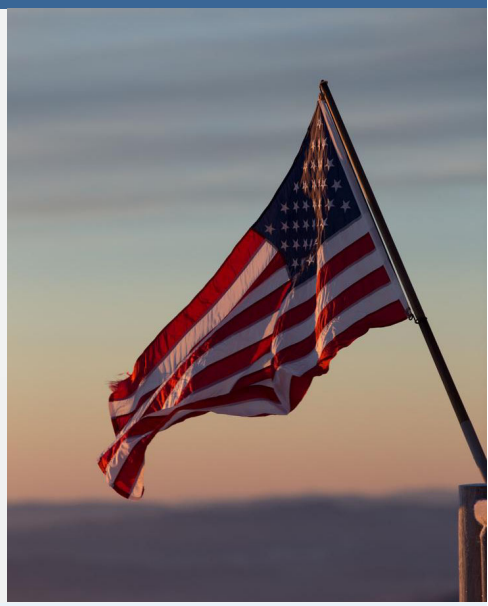
Taylor Swift : deepfakes et retrait de contenus illicites par X

X a suspendu les recherches des termes « Taylor Swift » en raison de la prolifération de « deepfakes » utilisant son image et sa voix. Ces contenus illicites doivent en effet être retirés rapidement par les sites Internet dès qu'ils en ont eu connaissance, conformément à l'article 6 de la LCEN. Afin de mieux identifier ces contenus, l'article 16 du Digital Service Act (DSA) exige désormais la mise en place de mécanismes de signalement plus simples.

FOCUS INTERNATIONAL

Interdiction des appels automatisés par le FCC

La Commission fédérale américaine des communications (FCC) a pris la décision de proscrire les appels automatisés utilisant des voix générées par intelligence artificielle (IA). Cette décision visent spécifiquement les appels automatisés employant des outils de clonage vocal d'IA. En effet, une enquête est en cours sur une potentielle tentative de perturber le scrutin actuel aux États-Unis, après qu'il a été constaté que des appels truqués usurpant la voix du président Joe Biden avaient été passés pour décourager les habitant du New Hampshire de voter aux primaires de l'État.



Air Canada condamnée en raison d'informations erronées données par son chatbot

Civil Resolution Tribunal, 2024 BCCRT 149, Moffatt v. Air Canada

Un client d'Air Canada avait réservé un vol auprès de la compagnie aérienne après le décès de sa grand-mère. Le chatbot présent sur le site internet de la compagnie lui avait affirmé qu'il pouvait, dans les 90 jours suivant son achat, demander un tarif spécial pour les voyageurs en deuil et il avait alors acheté un billet au tarif normal, pensant pouvoir obtenir le remboursement d'une partie de son billet.

Toutefois, après le voyage effectué, les employés d'Air Canada l'ont informé qu'il n'était pas possible de bénéficier de ce tarif après que le voyage avait eu lieu. Le Tribunal de résolution civile de la Colombie-Britanique a condamné Air Canada au versement d'un indemnité, considérant que l'entreprise était responsable des informations publiées sur son site internet, qu'elles proviennent d'une page web ou d'un chatbot.

ACTUALITÉS DONNEES PERSONNELLES

BREAKING NEWS

Entrée en vigueur du Data Act

Règlement UE fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données, 2022/0047(COD)

Le 11 janvier 2024, le Data Act est entré en vigueur. Il a pour objectif de compléter le Règlement (UE) 2022/868 du 30 mai 2022 sur la gouvernance des données applicable depuis le mois de septembre 2023 et met en place de nouvelles règles afin que les produits connectés soient fabriqués de manière à permettre à leurs utilisateurs, qu'ils soient professionnels ou consommateurs, d'accéder aux données générées par ces dispositifs, de les utiliser et de les partager avec des tiers.

Les thématiques prioritaires de contrôle de la CNIL pour 2024

Début février 2024, la CNIL a fait part de ses thématiques de contrôle prioritaires pour l'année 2024. Chaque année, elle oriente en effet ses contrôles sur des sujets à fort enjeux pour le public ou en lien avec l'actualité. En 2024, elle se concentrera sur :

- La collecte de données dans le cadre des Jeux Olympiques et Paralympiques ;
- La collecte en ligne des données des mineurs ;
- Les traitements de données dans le cadre des programmes de fidélité et tickets de caisse dématérialisés
- Les conditions de mise en œuvre du droit d'accès des personnes concernées.

Ces thématiques représenteront en moyenne 30% des contrôles effectués.

Collaboration de la CNIL et de l'autorité de la concurrence

Concurrence et données personnelles : une ambition commune

La CNIL et l'Autorité de la concurrence (ADLC) ont publié un document mettant en avant l'importance de leur collaboration. Ce document souligne le rôle crucial de la protection des données personnelles pour garantir une concurrence loyale. L'objectif d'une telle collaboration est de faire de la protection des données des consommateurs un avantage concurrentiel. L'ADLC et la CNIL ont prévu de se réunir périodiquement dans le cadre de séminaires pour développer leurs analyses sur des thématiques d'intérêt mutuel, telle que l'intelligence artificielle ou l'internet des objets, et d'approfondir leur compréhension des enjeux communs de régulation.

ACTUALITÉS DONNÉES PERSONNELLES

LES SANCTIONS DE LA CNIL

À l'encontre de YAHOO EMEA LIMITED

Délibération SAN-2023-024, 29 décembre 2023

Une sanction de 10 millions d'euros a été prononcée par la CNIL à l'encontre de YAHOO EMEA LIMITED. La CNIL, qui avait été saisie de 27 plaintes, a sanctionné le fait que des cookies étaient déposés sans accord de l'internaute. Par ailleurs, lorsqu'un utilisateur de la messagerie « Yahoo! Mail » souhaitait retirer son consentement au dépôt de cookies, la société le mettait en garde sur le fait qu'il ne pourrait plus accéder aux services proposés par la société et qu'il perdrait l'accès à sa messagerie, sans autre alternative proposée, ce que la CNIL condamne également.

À l'encontre de AMAZON FRANCE LOGISTIQUE

Délibération SAN-2023-021 du 27 décembre 2023

La CNIL a condamné AMAZON FRANCE LOGISTIQUE pour avoir mis en place un système de surveillance de l'activité et des performances des salariés excessivement intrusif. La CNIL a en effet relevé que la société utilisait des indicateurs sur l'activité et la performance des salariés, collectés à l'aide des scanners afin de gérer les stocks et les commandes dans ses entrepôts en temps réel, relevant un manquement au principe de minimisation des données et une illicéité des traitements. En effet, les indicateurs traités par la société menaient à une surveillance informatique excessive du salarié au regard de l'objectif poursuivi par la société. Enfin, la CNIL a considéré que les salariés et visiteurs extérieurs n'étaient pas correctement informés du traitement de leurs données et de la présence de systèmes de vidéosurveillance. Elle impose en conséquence de ces manquements une amende de 32 millions d'euros à AMAZON FRANCE LOGISTIQUE.

À l'encontre de TAGADAMEDIA

Délibération SAN-2023-025 du 29 décembre 2023

Le 29 décembre 2023, la CNIL a sanctionné la société TAGADAMEDIA d'une amende de 75 000 euros. Elle avait en effet décidé d'enquêter sur les pratiques des courtiers en données dans le cadre de sa thématique prioritaire de contrôle sur la prospection commerciale en 2022. Elle a ainsi relevé que TAGADAMEDIA collectait des données de prospects par le biais de formulaires sur ses sites de participation à des jeux-concours ou de tests de produits, mais que leur apparence ne permettait pas de recueillir un consentement libre, éclairé et univoquede l'utilisateur. Enfin, la CNIL relève un manquement dans la mise en œuvre du registre des activités de traitement. En effet, ce dernier, qui était partagé avec une seconde société, ne précisait pas laquelle agissait en qualité de responsable de traitement.

À l'encontre de PAP

Délibération SAN-2024-002 du 31 janvier 2024

La CNIL a prononcé une sanction de 100 000 euros à l'encontre de la société PAP qui édite le site pap.fr notamment pour avoir défini une durée de conservation de dix ans pour les données de certains comptes clients, sans que cette durée puisse être justifiée. La société informait par ailleurs les personnes au moyen d'une politique de confidentialité incomplète et imprécise. La CNIL a également relevé que les règles de complexité des mots de passe des comptes des utilisateurs du site étaient insuffisamment robustes et ne permettaient donc pas d'assurer la sécurité des données personnelles.

ACTUALITÉS DONNÉES PERSONNELLES

LES DONNÉES DE SANTÉ DANS LE VISEUR DE LA CNIL

Investigations de la CNIL sur la violation de données de santé

Fin janvier 2024, les société Viamedis et Lamerys, deux opérateurs gérant le tiers payant pour de nombreuses complémentaires santé et mutuelles, ont subi une cyberattaque qui aurait compromis les données personnelles de 33 millions de personnes. Les données concernées seraient celles concernant l'état civil, la date de naissance et le numéro de sécurité sociale, le nom de l'assureur santé ainsi que les garanties du contrat souscrit. À la suite de cet incident, la CNIL a initié des investigations afin de vérifier notamment si les mesures de sécurité mises en place avant et après l'attaque étaient conformes aux exigences du RGPD.

Affaire à suivre...

Mises en demeure par la CNIL de plusieurs établissements de santé

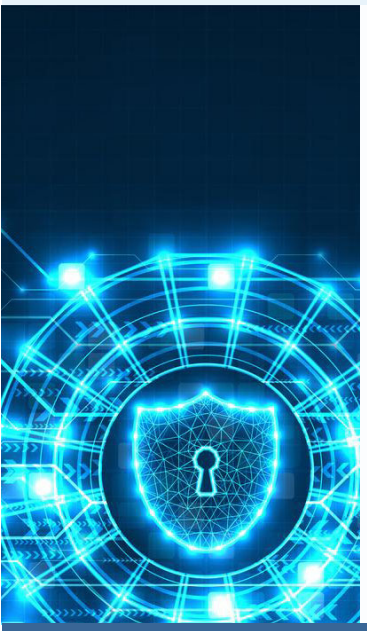
Après avoir été informée d'accès illégitimes aux données de patients contenues dans le dossier patient informatisé (DPI), la CNIL a réalisé 13 contrôles auprès d'établissements de santé de 2020 à 2024 qui ont révélé des lacunes dans les mesures de sécurité informatique et la gestion des habilitations, permettant notamment à des professionnels de santé non impliqués dans la prise en charge d'un patient d'accéder à des informations relatives à ce dernier. Dans ce contexte, la CNIL a mis en demeure plusieurs établissements de santé de renforcer la sécurité du DPI en mettant en place des accès au système par le biais d'une authentification robuste, en définissant des habilitations spécifiques pour que chaque professionnel de santé ou agent de l'établissement n'accède qu'aux dossiers dont il a à connaître et en assurant un traçage des accès au DPI.

Contestation de l'attribution du marché de l'hébergement d'EMC2 à Microsoft

Par une délibération de la CNIL en date du 21 décembre 2023, cette dernière a autorisé la création d'un entrepôt de données de santé dénommé « EMC2 », basé sur le traitement automatisé de données personnelles. Cet entrepôt permettra l'hébergement de données de santé issues de l'Assurance Maladie à l'échelle européenne ; sa création venant en réponse à un appel à projets lancé par l'Agence européenne des médicaments (EMA). La CNIL a confié pour une durée de trois ans l'hébergement de cet entrepôt à Microsoft Azure.

Cette délibération a été contestée devant le Conseil d'État par l'ONG Internet Society France, celle-ci espérant que cela contraigne les acteurs concernés à se réunir afin de trouver une solution équilibrée et respectueuse de la souveraineté technologique française et européenne.

ACTUALITÉS DONNÉES PERSONNELLES



Réparation du préjudice moral fondé sur la crainte d'un potentiel usage abusif de données personnelles

CJUE, 14 décembre 2023, C-456/22

Dans un arrêt du 14 décembre 2023, la Cour de justice de l'Union européenne (CJUE) a considéré que la crainte d'un potentiel usage abusif de données personnelles pouvait, à elle seule, constituer un dommage moral. En 2019, les médias avaient révélé l'existence d'une cyberattaque à l'encontre de l'Agence nationale des recettes publiques bulgare (NAP). Cet incident avait eu pour conséquence une fuite de données personnelles et leur publication sur Internet. De nombreuses victimes avaient alors introduit des actions en réparation de préjudices moraux découlant des craintes qu'elles avaient eu vis-à-vis d'une utilisation abusive potentielle de leurs données.

FOCUS INTERNATIONAL

La CNIL néerlandaise sanctionne Uber B.V. et Uber Technologies Inc.

Communiqué de presse de la Dutch Data Protection Authority (AP)

Après avoir reçu une plainte collective de l'association La Ligue des droits de l'Homme, représentant plus de 170 chauffeurs de la plateforme Uber – l'Autoriteit Persoonsgegevens – l'autorité néerlandaise de protection des données, en coopération avec la CNIL, a infligé le 11 décembre 2023 une amende de 10 millions d'euros pour plusieurs manquements à l'information des chauffeurs. En effet, les sociétés ne fournissaient pas aux chauffeurs les données sollicitées dans le cadre de leur droit d'accès dans un format accessible et ne rendaient pas suffisamment accessible le formulaire en ligne permettant l'exercice de ces droits. Les informations concernant le traitement des données étaient par ailleurs incomplètes au sein de la déclaration de confidentialité et cette dernière ne mentionnait pas de manière explicite le droit à la portabilité des données.

La CNIL italienne pourrait à nouveau interdire ChatGPT

À la suite d'une enquête ouverte par la Garante per la Protezione dei Dati Personali, l'autorité italienne de régulation de la vie privée, cette dernière a déclaré, sur la base des éléments en sa possession, que l'outil ChatGPT ainsi que les techniques utilisées pour recueillir les données des utilisateurs étaient contraires au RGPD. OpenAI peut soumettre ses demandes reconventionnelles concernant les violations alléguées dans un délai de 30 jours. La Garante per la Protezione dei Dati Personali précise qu'elle tiendra compte des travaux en cours au sein du groupe de travail mis en place par le Comité européen de la protection des données (EDPB) dans sa décision finale sur l'affaire.

NOUS CONTACTER

Stéphanie BERLAND
Avocate - Associée
IP-IT / Data / Media
sberland@steeringlegal.com
+33 6 81 45 05 01

Leslie HERAIL
Avocate
IP-IT / Data / Media
lherail@steeringlegal.com
+33 1 45 05 15 65

5 bureaux en France

- Angers
- Fort-de-France
- Marseille
- Paris
- Tours

7 bureaux dans le Monde

• **Emirats Arabes Unis** : Abu Dhabi et Dubai
• **Afrique** : Abidjan en Côte d'Ivoire et Niamey au Niger
• **Brésil** : Porto Alegre, Rio de Janeiro et Sao Paulo

STEERING LEGAL