ACTUALITÉS MAI-JUIN 2022

1. Espace européen de données de santé

La Commission européenne a récemment lancé l'espace européen des données de santé.
Un projet de règlement a ainsi été publié, le 3 mai dernier.
L'objectif affiché est de renforcer le pouvoir des citoyens européens sur leurs données de santé, tant dans leur pays d'origine, que dans d'autres Etats membres et de favoriser la recherche et l'innovation.
A cet égard, la Commissaire à la santé et à la sécurité alimentaire, Madame Stella Kyriakides a déclaré que « *l'espace européen des données de santé change fondamentalement la donne pour ce qui est de la transformation numérique des soins de santé dans l'UE. Ces données, auxquelles il sera possible d'accéder dans le cadre de solides garanties en matière de sécurité et de respect de la vie privée, constitueront également une mine d'or pour les scientifiques, les chercheurs, les innovateurs et les décideurs travaillant sur le prochain traitement vital* ».
Il est prévu que les citoyens aient un accès immédiat, gratuit et simplifié à leurs données sous forme électronique qu'ils pourront partager avec d'autres professionnels de la santé, étant précisé qu'ils seront en mesure d'ajouter des informations, de rectifier des données erronées ou de restreindre l'accès à leurs données, mais également d'obtenir des informations sur la manière dont leurs données sont utilisées ainsi que sur les finalités. Cela passera, non seulement, par une standardisation des dossiers médicaux électroniques et documents de santé, mais également par une interopérabilité et un renforcement en termes de sécurité notamment par la mise en place de mécanismes de certification des systèmes.
Enfin, les Etats membres devront intégrer un programme « *MaSanté@EU* » pour procéder au partage de données de santé pour des soins primaires.
En matière de recherche et utilisation secondaire des données de santé, l'accès aux données ne sera *a priori* autorisé que si les données demandées sont utilisées à des fins particulières, dans des environnements fermés et sécurisés et sans que l'identité des personnes ne soit révélée.

Pour plus d'informations: A European Health Data Space for people and science (europa.eu)

2. Réforme britannique sur le droit des données personnelles

Par communiqué du Ministère britannique au numérique, à la culture, aux médias et au sport, publié le 17 juin dernier, le Gouvernement britannique a apporté des précisions sur les changements qu'il souhaite apporter à la régulation de la protection des données personnelles.
Déjà en 2021, il avait évoqué son souhait de se détacher du Règlement Général sur la Protection des Données (RGPD).
En termes de cookies, le système de « *pop-ups* » (fenêtres s'affichant lors de la navigation sur un site web) serait remplacé par un modèle d'« *opt-out* » impliquant un consentement acquis par défaut.
Dès lors, l'utilisateur choisirait directement dans les paramètres de son ordinateur s'il accepte ou non que les sites puissent collecter ses données grâce aux cookies, avec une possibilité laissée pour la création d'une liste d'exception.
D'autres modifications seront *a priori* apportées par rapport au RGPD, parmi lesquelles la restructuration de l'Autorité britannique de protection des données, l'utilisation de données au titre de la recherche scientifique, etc.

Si le Royaume-Uni était considéré jusqu'à présent, par l'Union Européenne, comme disposant d'un niveau de protection adéquat en matière de protection des données personnelles, il n'est pas à exclure que cela soit remis en cause, notamment par le biais de la clause de caducité qui nécessitera une réévaluation et un renouvellement de la décision d'adéquation en 2024.

3. Bipartisan American Data Privacy and Protection Act

Un groupe bipartisan de législateurs américains a récemment dévoilé un projet de discussion portant sur un avant-projet de loi fédérale sur la protection des données (*American Data Privacy and Protection Act*). Celui-ci vise à mettre en place un ensemble de règlementations fédérales destinées à protéger les données personnelles des américains.
Cet avant-projet de loi a pour objectif de redonner aux américains un pouvoir de contrôle notamment sur l'accès et le partage de leurs données par les plateformes et courtiers.
Il prévoit, en outre, différents seuils en fonction de la taille des entreprises assujetties.
De même, y sont prévues des dispositions protectrices des mineurs, des limites à la publicité ciblée, ainsi qu'un droit d'action privé, bien que ce dernier soit relativement limité. D'autres exigences en termes de minimisation et de réduction des données y sont également inclues.
La « *Federal Trade Commission* » devrait être chargée de faire respecter ces nouvelles exigences.
Se pose désormais la question d'une éventuelle prochaine adoption.

4. Règlement pour la protection des données personnelles et compétence des associations de consommateurs

L'Union fédérale des centrales et associations de consommateurs (association allemande de défense des consommateurs) a intenté, devant les juridictions allemandes, contre la plateforme Meta Plateforms Ireland, une action en cessation de violation des droits issus du RGPD et des dispositions relatives à la lutte contre la concurrence déloyale et la protection des consommateurs.
Elle lui reprochait notamment la violation de ces droits dans le cadre de la mise à disposition des utilisateurs de jeux gratuits fournis par des tiers.
La compétence de cette Union pour agir, au sens du RGPD, et défendre les droits personnels de ses membres a été soulevée devant la Cour fédérale de justice allemande, laquelle a elle-même saisi la Cour de Justice de l'Union européenne (CJUE) d'une question préjudicielle.
La question portait d'une part sur la recevabilité d'une action en l'absence de mandat et, d'autre part, sur la nécessité ou non d'identifier au préalable individuellement la personne concernée par cette violation.
La CJUE y a répondu (à la lumière de l'article 80 paragraphe 2 du RGPD) en jugeant que le RGPD permet à une association de défense des intérêts des consommateurs d'agir en justice y compris en l'absence de mandat conféré à cette fin. De plus, cette action est possible indépendamment de la violation de droits concrets des personnes concernées, contre l'auteur présumé d'une atteinte à la protection des données. La CJUE a notamment relevé que cette association relevait de la notion d'« *organisme ayant la qualité pour agir* » au sens du RGPD dans la mesure où elle poursuit un objectif d'intérêt public qui consiste à assurer les droits des consommateurs. Or, la violation de règles relatives à la protection des consommateurs ou aux pratiques commerciales déloyales peut être connexe à la violation de règles relatives à la protection des données.
CJUE, 28 avr. 2022, aff. C-319/20, Meta Plateforms Ireland

5. Cookie Walls

La pratique des « *cookie Walls* » (littéralement, murs de traceurs) consiste à conditionner l'accès à un service à l'acception préalable, par les utilisateurs, du dépôt de traceurs sur leur terminal.
De nombreux sites internet ont instauré, comme alternative au refus des utilisateurs de consentir à ce dépôt, une contrepartie financière (« *paywall* »).
Un paywall oblige ainsi les internautes à verser une somme d'argent pour accéder à un site dont ils auraient refusé le dépôt de cookies et traceurs sur leur terminal.
L'autorité de protection des données française (CNIL) vient récemment de publier ses premiers critères permettant d'évaluer la légalité de cette pratique, dont il y a lieu de rappeler que la plus haute juridiction administrative française (le Conseil d'Etat) avait jugé, en 2020, que l'exigence d'un consentement libre ne pouvait pas justifier une interdiction générale de cette pratique et nécessitait une appréciation au cas par cas.
Ainsi, s'agissant des cookie Walls, la CNIL a estimé que leur légalité doit s'apprécier « *en tenant compte de l'existence d'alternative(s) réelle(s) et satisfaisante(s) proposée(s) en cas de refus des traceurs* ». Elle recommande plus particulièrement la proposition d'une « *alternative réelle et équitable* » avec une « *facilité d'accès pour l'utilisateur à cette alternative* ».
La CNIL a ainsi considéré qu'il pouvait y avoir un déséquilibre en cas d'exclusivité de l'éditeur sur les contenus ou services proposés ou encore lorsque l'internaute n'a pas ou peu d'alternatives au service.
S'agissant plus précisément de la pratique des « *paywall* », elle a souligné que la contrepartie monétaire ne doit toutefois pas être de nature à priver les internautes d'un véritable choix, le tarif fixé devant être raisonnable.
Quant aux sites imposant à l'utilisateur la création d'un compte, la CNIL a indiqué que les éditeurs devront s'assurer qu'une telle obligation est justifiée par rapport à l'objectif visé.
En outre, en cas de conditionnement de l'accès du site au consentement à une ou plusieurs finalités, « *l'éditeur devra démontrer que son cookie Wall est limité aux finalités qui permettent une juste rémunération du service proposé* ».

6. Clauses contractuelles types chinoises

Le régulateur chinois de la protection des données (« *The Cyberspace administration of China* ») a publié un projet de clauses contractuelles-types destinées à encadrer les transferts de données vers l'extérieur. Ce dernier est ouvert au public, pour commentaires jusqu'au 29 juillet prochain.

À suivre.

7. Autorités de protection des données et autres Autorités

APD

- **LCB-FT, lettre du Comité Européen de la protection des données (CEPD)**

Le CEPD, qui réunit les autorités européennes de protection des données, a adressé, aux législateurs européens, une lettre publique au terme de laquelle ils estiment essentiel une meilleure prise en compte des principes posés par le RGPD dans l'élaboration de la législation visant à renforcer les règles européennes de lutte contre le blanchiment de capitaux et le financement du terrorisme.
Selon lui, il importe de :

- préciser les conditions de traitement des données personnelles dans les textes européens ;
- impliquer davantage le CEPD dans l'élaboration des textes ;
- prévoir des garanties pour le traitement des données sensibles et des données relatives à des condamnations pénales ;
- encadrer les sources de données utilisées par les organismes concernées.

➢ **Autorité de protection des données française - CNIL**

- Transmission de données de prospects à des fins commerciales sans consentement

La Commission Nationale Informatique et Liberté a récemment mis en demeure plusieurs sociétés pour avoir transmis à des partenaires des données personnelles de prospects sans recueil de consentement. Ces sociétés disposent d'un délai de 3 mois pour se mettre en conformité avec la règlementation.

- Google Analytics

42 plaintes à l'encontre de médias ont été déposées auprès de la CNIL en raison de l'utilisation du cookie de mesure d'audience Google Analytics. Rappelons pourtant que l'utilisation de Google Analytics est illégale, dans le pays voisin, depuis le 10 février dernier.

- Mise en demeure de plusieurs communes

La CNIL a récemment mis en demeure 22 communes françaises récalcitrantes à désigner un Délégué à la Protection des Données. En effet, aux termes de l'article 37 du Règlement Général sur la Protection des Données, les responsables de traitement et sous-traitants sont tenus de désigner un Délégué à la Protection des Données lorsque le traitement est effectué par une autorité publique ou un organisme public à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle.
Ces communes disposent désormais d'un délai de 4 mois pour se mettre en conformité.

- Précisions sur les enregistrements de conservations téléphoniques pour établir la preuve de la formation d'un contrat

La CNIL a notamment apporté des précisions sur les conditions dans lesquelles cet enregistrement peut être réalisé, mais également sur les garanties à apporter.
Ainsi un tel enregistrement est autorisé sous réserve d'être nécessaire (le responsable de traitement devra démontrer qu'il ne dispose pas d'autres moyens pour prouver que le contrat a été conclu).
La CNIL distingue donc les contrats pouvant être conclus à l'oral de ceux devant l'être à l'écrit.
S'agissant des contrats conclus à l'oral, l'enregistrement devra néanmoins (si l'enregistrement semble possible) respecter le principe de minimisation des données.
Dès lors, de tels enregistrements ne pourront être permanents ou systématiques. De même, seules les conversations portant sur la conclusion d'un contrat par voie téléphonique pourront être enregistrées. En outre, celles-ci ne pourront être conservées qu'en l'absence d'une autre modalité de preuve. Tel ne sera pas le cas, par exemple, d'un contrat conclu par voie téléphonique mais faisant l'objet d'une confirmation écrite.
L'enregistrement de la conversation téléphonique ne pourra par ailleurs pas être déclenché par défaut, pour tous les appels et toutes les conversations.
S'agissant de la base légale relative à l'exécution d'un contrat, il conviendra, pour s'en prévaloir, de bien informer les personnes concernées de l'existence d'autres moyens de conclure le contrat.

- Prospection commerciale

La société TOTALENERGIES a été sanctionnée d'une amende d'un million d'euros pour non-respect de ses obligations en matière de prospection commerciale et de droits des personnes. Cette sanction fait suite à plusieurs plaintes adressées à la CNIL par des personnes ayant rencontré d'importantes difficultés lors de demandes d'accès à leurs données et d'oppositions à recevoir des appels de prospection commerciale. S'agissant plus particulièrement du manquement à l'obligation des personnes de s'opposer à de la prospection commerciale, il a été constaté que la société proposait, sur son site, un formulaire de souscription à un contrat d'énergie dans lequel le souscripteur donnait son accord pour l'utilisation de ses données à des fins de prospection sans toutefois pouvoir s'y opposer.

- **Autorité de protection des données italienne**

  - Accès non autorisé à des données

L'Autorité de protection des données italienne a sanctionné, d'une amende de 50.000 euros, l'agence nationale pour l'assurance contre les accidents du travail (Istituto Nazionale Assicurazione Infortunio sul Lavoro (INAIL).
Cette amende fait suite à des accès non autorisés à des données de travailleurs, en particulier à des données concernant leur santé (maladies professionnelles) et leurs accidents de travail. L'Autorité a relevé, à cet égard, qu'aucune mesure technique et organisationnelle n'avait été mise en place pour assurer un niveau de sécurité approprié à la lumière des risques découlant du traitement en question.

  - Google Analytics

Après les Autorités de protection des données autrichienne et française, c'est au tour de l'autorité italienne de considérer qu'un site web utilisant Google Analytics, sans les garanties définies par le Règlement pour la protection des données, enfreint la loi sur la protection des données en ce qu'il transfère des données d'utilisateurs aux Etats-Unis, pays sans niveau de protection adéquate.

Autres autorités

- **Cour de Justice de l'Union Européenne (CJUE) et précisions apportées sur les réponses aux droits d'accès des personnes concernées**

L'Avocat Général de la CJUE, M. Giovanni Pitruzzella, a récemment rendu un avis concernant l'interprétation du droit d'accès, tel que prévu à l'article 15 du Règlement général sur la protection des données (RGPD). Cet avis porte plus précisément sur le droit d'une personne d'accéder aux informations concernant les destinataires et catégories de destinataires et fait suite à la demande d'un résident autrichien adressée à la poste afin d'obtenir la liste de tous les destinataires auxquels ses données personnelles avaient été divulguées. La poste avait répondu à cette demande en lui adressant un aperçu des catégories de destinataires. Contestant cette réponse devant les juridictions autrichiennes, le requérant faisait valoir qu'il aurait dû recevoir une liste de destinataires spécifiques conduisant la Cour d'appel à soumettre une question d'interprétation à la CJUE.
Dans le cadre de son avis, l'Avocat Général a ainsi, à titre liminaire, exposé, qu'eu égard à la formulation retenue, l'article 15 paragraphe 1 point c) du RGPD ne permettait pas d'apporter, à lui seul, une réponse à la question posée (les termes « *destinataires* » et « *catégories de destinataires* » sont utilisés de façon neutre, sans ordre de priorité et sans qu'il soit possible de savoir si un choix peut être fait ou qui pourrait le faire).
Cela dit, il a toutefois considéré que la structure de l'article suggère qu'une personne concernée puisse choisir entre les deux types d'information et que cette interprétation est soutenue par le considérant 63 qui ne permet pas, en revanche, aux responsables de

traitement de restreindre le droit aux seules catégories de destinataires. L'Avocat Général a également souligné que l'objectif du droit d'accès est bien de permettre aux personnes concernées de connaître les activités de traitement de leurs données et de vérifier la légalité du traitement y compris le fait qu'elles n'aient été divulguées qu'à des destinataires autorisés. Or, selon lui, la limitation des informations aux catégories de destinataires ne permettrait pas aux personnes concernées d'atteindre cet objectif. De plus, les informations fournies en vertu d'une demande de droit d'accès peuvent également être pertinentes pour l'exercice d'autres droits (ex. droit d'opposition). Enfin, le RGPD exige que les responsables de traitement, lors d'une demande de droit d'accès identifient les destinataires spécifiques. Deux circonstances sont toutefois prévues permettant au responsable de traitement de ne répondre qu'en fournissant des informations limitées à des catégories de destinataires :

- lorsque cela est matériellement impossible de fournir des détails spécifiques sur les destinataires ;
- Si la demande est manifestement infondée ou excessive.

- **Federal Trade Commission**

  La plateforme Twitter a écopé d'une pénalité de 150 millions de dollars en raison de l'utilisation des données personnelles de ses utilisateurs liées à l'authentification à deux facteurs à des fins publicitaires.

  Plus précisément, l'agence fédérale chargée d'appliquer le droit de la consommation et contrôler les pratiques anticoncurrentielles (Federal Trade Commission – FTC) lui a reproché d'avoir, entre 2013 et 2019, utilisé les adresses emails et les numéros de téléphones des utilisateurs dans ses outils publicitaires sans les en notifier.

  Le Département de Justice a, à cet égard, déclaré « *Twitter a dit à ses utilisateurs qu'il recueillait leurs numéros de téléphone et leurs adresses électroniques à des fins de sécurité des comptes, mais n'a pas révélé qu'il utiliserait également ces informations pour aider les [...] entreprises à envoyer des publicités ciblées aux consommateurs. La plainte allègue en outre que Twitter a faussement prétendu se conformer aux cadres du bouclier de protection de la vie privée Union européenne-États-Unis et Suisse-États-Unis, qui interdisent aux entreprises de traiter les informations des utilisateurs d'une manière qui n'est pas compatible avec les fins autorisées par ces derniers* ».

  Il en a notamment résulté une violation de l'accord conclu en 2011 avec le FTC lui interdisant de faire des fausses déclarations sur l'utilisation des informations des contacts des particuliers.

- **Tribunal de commerce de Paris**

  Par décision du 28 mars 2022, Google a été condamné à s'acquitter d'une amende de 2 millions d'euros en plus d'une obligation de modifier, dans un délai de 3 mois, ses conditions contractuelles considérées comme étant déséquilibrées.

  Cette condamnation faite sur le fondement de l'article L. 442-6 du Code de commerce français (sur les pratiques restrictives de concurrence qui sanctionnent les abus dans les relations commerciales entre entreprises) fait suite à une enquête menée, entre 2015 et 2016, par le régulateur français en matière de concurrence, consommation et répression des fraudes. Cette dernière portait sur les conditions commerciales liant Google aux développeurs proposant sur le marché français leurs produits sur la plateforme Play Store. En effet, il lui a été reproché d'imposer des conditions contractuelles soumettant les développeurs à des obligations créant un déséquilibre significatif. Le Tribunal de Commerce a notamment pris en compte la position de Google Play sur le marché français.

- **Conseil d'Etat et validation de la sanction de l'autorité de protection des données française contre Amazon**

Amazon devra donc s'acquitter de l'amende de 35 millions d'euros prononcée, à son encontre, par l'autorité de protection des données française. Telle est la décision du Conseil d'Etat dans un arrêt en date du 27 juin 2022.
Pour rappel, Amazon avait été condamnée en raison de dépôts de cookies publicitaires sur les ordinateurs des utilisateurs de sa plateforme e-commerce sans possibilité de refus.
Conseil d'État (conseil-etat.fr)