ACTUALITÉS SEPTEMBRE 2021

1. **Nouvelles discussions en cours entre les Etats-Unis et l'Union Européenne pour un nouvel accord de transfert de données**

A la suite de l'invalidation du Privacy Shield par la CJUE, des négociations ont débuté le 13 septembre 2021 avec les Etats-Unis (délégation du Conseil de Sécurité) s'agissant de la problématique des transferts de données.

L'enjeu du côté européen est de parvenir à convaincre les Etats-Unis de mettre en place une procédure permettant à un Européen de pouvoir contester efficacement les mesures de surveillance américaines notamment mises en place par le *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act).

Dans l'attente d'un accord des solutions temporaires ont été mises en place - ex. contrats prêts à l'emploi- mais qui semblent s'avérer insuffisantes.

L'Autorité Irlandaise a ainsi récemment adressé à Facebook Irlande un avant-projet d'ordonnance (qui pourrait en réalité concerner toutes les entreprises des nouvelles technologies tech qui sont soumises aux lois américaines soit environ 5 300). Côté américain, un projet de loi bipartisan (*Social Media Privacy Protection and Consumer Rights* Act) a été déposé aux Etats-Unis sur la confidentialité des données.

À suivre !

2. **Échanges d'informations financières à des fins d'enquêtes pénales : finalisation de la transposition en France de la directive (UE) 2019/1153**

4 textes promulgués le 25 août 2021 ont achevé la transposition, par l'ordonnance 2021-958 du 19 juillet 2021, de la directive (UE) 2019/1153 du 20 juin 2019 (il s'agit des décrets 2021-1112 ; 1113 plus deux arrêtés).
Ces textes permettent de fixer les règles facilitant l'utilisation d'informations financières et d'une autre nature aux fins de la prévention ou de la détection de certaines infractions pénales, d'enquêtes ou de poursuites en la matière.
Pour rappel, la directive (UE) 2019/1153 a pour objectif de faciliter l'accès et les échanges d'informations financières permettant de lutter contre les infractions graves de criminalité en bande organisée (trafic d'êtres humains, de drogue, d'armes), de délinquance financière (corruption, blanchiment de capitaux) et de financement du terrorisme et s'inscrit, de ce fait, dans le prolongement de la 5ème directive.
La directive (UE) 2019/1153 prévoit notamment l'accès des autorités répressives aux informations contenues dans le fichier national des comptes bancaires (FICOBA) mais aussi à celles détenues par TRACFIN. De même, il est prévu une facilitation des échanges entre les autorités nationales et EUROPOL et la définition des modalités d'échanges assorties de garanties relatives à la protection des données.
NB : Ces mécanismes étaient en réalité déjà possibles grâce au cadre juridique français de sorte que seuls quelques aménagements à la marge ont, en réalité, été réalisés.

Pour revenir rapidement sur les apports des décrets 2021-1112 et 1113 : le premier définit les modalités pratiques d'échanges d'informations financières ou relatives aux comptes entre autorités compétentes au moyen de communication électronique sécurisée. Il revient par

ailleurs sur les obligations de traçabilité des échanges avec la tenue d'un registre imposée aux différentes autorités pour une durée de 5 ans.
Le second, prévoit la tenue de statistiques par le Conseil d'orientation de la lutte contre le blanchiment de capitaux et le financement du terrorisme pour transmission à la Commission Européenne ainsi que les conditions d'accès à FICOBA par les agents de l'Agence de gestion et de recouvrement des avoirs saisis et confisqués (*cette agence est un établissement public dont le rôle est notamment d'aider, de conseiller et d'orienter les magistrats et enquêteurs en matière de saisies et de confiscations et d'améliorer le traitement judiciaire des saisies et des confiscations en matière pénale*).

3. Proposition de Directive « crédit aux consommateurs »

La Directive « crédit aux consommateurs » devrait, si elle était adoptée, remplacer la Directive 2008/48 CE relative aux contrats de crédit aux consommateurs et permettre une adaptation des règles actuelles relatives à la numérisation.
Le passage au numérique a modifié de façon importante tant le processus de prise de décision et les habitudes des consommateurs (ces derniers recherchent des procédures simples et rapides pour obtenir leur crédit) que le secteur des prêts ce qui a contribué à l'apparition de nouveaux acteurs (plateforme de prêts entre particuliers) et de nouveaux produits.
La proposition de Directive vise ainsi à appréhender les problématiques en lien avec la protection des données personnelle spécifiques aux pratiques du marché aux crédits à la consommation (utilisation de sources de données non-conventionnelles pour évaluer la solvabilité).
Le Comité Européen à la Protection des Données a récemment rendu un avis sur la proposition de Directive et a notamment invité le législateur à préciser davantage les catégories de données ne pouvant pas être utilisées pour l'évaluation de la solvabilité (ex. traitement des données provenant des réseaux sociaux, données de santé).
Il recommande en outre d'étendre cette interdiction à l'utilisation de toute catégorie particulière de données à caractère personnel en vertu de l'article 9 du RGPD, aux informations concernant le comportement de navigation en ligne des individus et préconise un encadrement du rôle et des responsabilités des bases de données de crédit ou de tiers fournisseurs de crédits-scores (évaluation des risques clients).

4. Récapitulatif de décisions rendues par la CEDH publiées au Bulletin d'Information de la Cour de Révision de septembre 2021

- **L'atteinte à la protection des données personnelles établie sur le fondement de l'article 8 de la CEDH consacrant le droit au respect de la vie privée**

  - *Au sujet de la conservation sans limite de durée et possibilité de réexamen de la situation d'un profil ADN, d'empreintes digitales et d'une photographie d'une personne reconnue coupable d'une infraction mineure* ***(CEDH, 13 fév. 2020, Gaughran c/ Royaume-Uni)*** *:*

    La Cour y voit une atteinte disproportionnée au droit au respect de la vie privée, compte tenu du caractère disproportionné de la conservation caractérisée par l'absence d'examen de la gravité de l'infraction commise et de la nécessité de conserver indéfiniment les données en question. La CEDH précise que l'État bénéficiait d'une marge d'appréciation un peu plus ample concernant la conservation des empreintes digitales et de photographies laquelle était en l'espèce insuffisante pour que la conservation des données soit considérée comme proportionnée (absence de garanties suffisantes et de possibilité réelle d'examiner la matière litigieuse).

- *Sur l'existence d'une obligation légale pour les opérateurs de téléphonie mobile de recueillir des données d'utilisateurs de cartes SIM prépayées et les tenir à disposition des autorités* CEDH ***(CEDH, 30 janv. 2020, Breyer c/ Allemagne)***

  La Cour n'y voit aucune violation de l'article 8.

- *Prélèvement d'un échantillon de salive aux fins de test ADN non prévu par la Loi au sens de l'article 8 de la CEDH* ***(CEDH, 14 avr. 2020, Dragan Petrovic c/ Serbie)*** *:*

  La Cour retient qu'en l'occurrence, les dispositions du code de procédure pénale au moment des faits ne prévoyaient que les prélèvements sanguins ou d'autres procédures médicales.

- **La vidéosurveillance**

  - *La surveillance permanente de détenus dans leurs cellules* ***(CEDH 2 juil. 2019, Gorlov et a. c/Russie)*** *:*

    Si la Cour y voit une atteinte à l'article 8, elle reconnaît néanmoins la possibilité de surveiller certaines zones d'établissements pénitentiaires ou certains détenus d'une façon permanente. En l'espèce, elle avait considéré que le cadre juridique russe n'était pas suffisamment clair et précis ou encore détaillé pour permettre d'offrir une protection appropriée contre l'ingérence arbitraire des autorités dans le droit au respect de la vie privée. En l'occurrence, le requérant n'a pas bénéficié d'un degré minimal de protection attendu dans une société démocratique.

  - *La surveillance de masse et la détection de menaces pesant sur la sécurité nationale des États* ***(CEDH 25 mai 2021, Centrum for rattvisa c/ Suède)***

    L'interception de masse à des fins de détection de menaces pesant sur la sécurité nationale des États a été reconnue par la Commission de Venise de Conseil de l'Europe. La Cour retient que dans les conditions actuelles aucune solution ou combinaison de solutions ne serait suffisante pour remplacer cette activité et qu'elle n'a pas pour tâche de prescrire un modèle pour le renseignement électromagnétique des États-Membres.
    Concernant le modèle suédois (qu'elle a considéré dans son ensemble) elle a ainsi retenu que le système d'interception de masse est fondé sur des règles juridiques détaillées avec une portée délimitée et offrant des garanties. Cela étant, la Cour a relevé 3 carences relatives à l'absence de règle claire concernant la destruction des éléments interceptés qui ne contiennent pas de données personnelles **(i)**, au fait que ni la loi ni aucun autre texte n'énonce l'obligation de prendre en compte les intérêts liés à la vie privée lorsqu'une décision de partage de renseignements avec des partenaires étrangers est adoptée **(ii)** et à l'absence de contrôle *a posteriori* effectif **(iii)**.
    Concernant la seconde carence, elle relève plus précisément que celle-ci pourrait permettre une transmission mécanique vers l'étranger d'informations dont la communication porte gravement atteinte au droit au respect à la vie privée ou au droit au respect de la correspondance « *qui ne présenteraient pourtant que très peu d'intérêt en termes de renseignement* ». En outre, la Cour considère qu'aucune obligation juridiquement contraignante n'impose au Service de renseignements suédois spécialisé dans le renseignement d'origine électromagnétique d'analyser les garanties offertes par le destinataire étranger des renseignements afin de déterminer si elles sont d'un niveau minimum acceptable. S'agissant de l'absence de contrôle *a posteriori*, la Cour retient que

« *le double rôle de l'Inspection et l'impossibilité pour les particuliers d'obtenir des décisions motivées sous quelque forme que ce soit en réponse à leurs plaintes ou interrogations concernant l'interception en masse de communications affaiblissent le mécanisme de contrôle a posteriori dans une mesure qui engendre des risques pour le respect des droits fondamentaux des personnes concernées. (…) l'absence de contrôle effectif au dernier stade de l'interception n'est pas conciliable avec la situation constatée par la Cour, où l'intensité de l'ingérence faite dans l'exercice des droits protégés par l'art. 8 augmente au fur et à mesure que le processus avance, et elle ne satisfait pas à l'exigence de « garanties de bout en bout* ».

5. Royaume-Uni et protection des données personnelles

Peu de temps après les décisions d'adéquation rendues, le 28 juin 2021, par la Commission Européenne vis-à-vis du Royaume-Uni (RU), ce dernier a annoncé son intention de s'écarter de la règlementation européenne jugée trop stricte avec pour objectif d'entrer dans une ère axée sur la croissance et l'innovation économique. Le Gouvernement Britannique a ainsi annoncé son intention de modifier l'encadrement de la collecte des cookies (suppression des bannières de demandes de collecte à l'étude) et de signer de nouveaux partenariats sur l'adéquation des données, ainsi que leurs transferts notamment avec l'Australie, la Corée du Sud et les USA. Affaire à suivre !

6. Enquêtes et sanctions prononcées par les autorités de contrôle européennes

➢ France

Enquête

Une enquête a été ouverte conjointement par la CNIL et la Préfecture de Police à la suite du piratage de systèmes informatiques de l'AP-HP (notamment un service de partage de fichiers permettant la transmission d'informations pour le « *contact tracing* ») qui a conduit au vol de fichiers contenant des données médicales de 1,4 million de personnes. Cette attaque qui a eu lieu au cours de l'été a été confirmée le 12 septembre 2021. Ont ainsi été dérobés l'identité, le numéro de sécurité sociale, les coordonnées des personnes testées et les caractéristiques et résultat du test.

Sanctions

- Sanctions prononcées par la CNIL à l'encontre du Figaro (50.000 euros) en raison de dépôts de cookies publicitaires par des partenaires sur le site lefigaro.fr sans consentement préalable des internautes et d'AG2R (1,5 million) du fait de manquements en termes de durées de conservation et de manquements aux règles d'information des personnes.

- Sanction d'un montant de 3.000 euros prononcée par la CNIL à l'encontre de la Société Nouvelle de l'Annuaire Français (SNAF) pour non-respect du droit des personnes concernées. 16 plaintes avaient été reçues par la CNIL entre 2018 et 2019.
  Ont été relevés par la CNIL les manquements suivants :
  - Manquement à l'obligation de respecter les demandes de rectification de données ;
  - Manquement à l'obligation de respecter les demandes d'effacement des données ;
  - Manquement à l'obligation de mettre en œuvre un registre des activités de traitement ;

- Manquement à l'obligation de coopérer avec la CNIL.

➢ **Irlande**

Enquête

Une enquête a été ouverte à l'encontre de Tik Tok par la Data Protection Commission (CNIL irlandaise). Le réseau est en effet soupçonné d'envoyer de façon irrégulière des données en Chine et de ne pas suffisamment protéger celles des mineurs. Un porte-parole de l'application a indiqué « *s'appuyer sur des mécanismes homologués pour les données transférées hors d'Europe* ». De tels soupçons avaient déjà conduit le gouvernement américain à essayer de bannir l'application des Etats-Unis.
Concernant par ailleurs la protection des données de mineurs le réseau se défend en indiquant avoir mis en œuvre d'importantes mesures, les comptes des moins de 16 ans ayant été placés d'office en privé en janvier 2021.
En outre depuis 2020, la CNIL et son homologue néerlandaise enquêtent sur la gestion de la vie privée par Tik Tok.

7. Actualités du monde numérique

Europe

❖ **La plateforme de partage de documents Tilkee certifiée pour les données de santé**
La solution de partage de documents sécurisée et de signature électronique basée à Lyon a obtenu deux nouvelles certifications : l'une portant sur la gestion de la sécurité des systèmes d'information (ISO 27001) et l'autre sur l'hébergement de données de santé. L'entreprise a par ailleurs obtenu la certification AFNOR AFAQ protection des données personnelles.

❖ **France : 85 % de l'objectif des démarches numériques atteint**
En termes de chiffres, cela représente 215 sur les 250 formalités « essentielles à la vie quotidienne ». S'agissant de l'avancement du plan de numérisation des services publics, seront prochainement mis à la disposition des usagers – la possibilité d'inscrire leurs enfants au collège et au lycée en ligne ; - la demande d'une aide juridictionnelle ; - la possibilité d'établir une procuration en ligne, - la numérisation des demandes de permis de construire.
Niveau budget 7 millions d'euros ont été piochés dans le budget d'un milliard du plan de relance de l'économie. Un bémol relevé : l'accessibilité des personnes handicapées aux démarches en ligne.

❖ **Ouverture du code source : France Connect**
Le Ministre de la Transformation et de la Fonction Publique a annoncé l'ouverture du code source de France Connect à compter de novembre 2021. Un tel partage avait déjà eu lieu avec l'algorithme de la taxe d'habitation, de l'impôt sur le revenu, du calculateur des impôts ou de certains éléments de Tous Anti Covid.

Reste du monde

❖ **L'Australie, la Malaisie, Singapour et l'Afrique du Sud vont tester des paiements transfrontaliers en monnaie numérique**
Les banques centrales de ces quatre pays se sont engagées à mettre en œuvre des solutions pour permettre de réaliser des paiements transfrontaliers à l'aide d'une future monnaie numérique.

Un test d'interopérabilité sera mis en œuvre, étant précisé que les membres du G20 ont également indiqué qu'ils souhaitaient établir des normes pour faciliter les paiements transfrontaliers.