ACTUALITÉS JUILLET-AOÛT 2022

1. **Approbation du Digital Services Act (DSA) et du Digital Markets Act (DMA) par le Parlement européen**

   Les DSA et DMA, ayant respectivement vocation à permettre la modération des contenus numériques et la régulation des pratiques anticoncurrentielles en luttant, notamment, contre les abus de position dominante, ont finalement été définitivement approuvés le 5 juillet dernier.
   Ces deux règlements doivent encore être approuvés par le Conseil de l'Union européenne.
   Une fois cette étape passée, ils devraient rapidement entrer en vigueur et être publiés au Journal officiel de l'Union européenne.
   Un court délai d'adaptation est prévu pour permettre aux acteurs concernés de se conformer à leurs obligations en vertu de ces deux textes. Certains estiment à cet égard que celles-ci ne seront pas suffisantes face à la puissance des GAFAM (géants du Web tels que Google, Apple, Facebook).

2. **Directive NIS 2 et renforcement des exigences envers les entreprises privées et le secteur public**

   Pour faire face aux cybermenaces toujours plus nombreuses, l'Union européenne s'était dotée, en 2016, d'une directive « *Network and Information System Security* » (Directive NIS) (entrée en vigueur en 2018), dont le texte devrait être prochainement révisé. Un accord politique a en effet été trouvé en ce sens, au printemps 2022, entre la Commission, le Parlement et le Conseil européen.
   Des milliers d'entreprises devraient ainsi être contraintes de renforcer leur niveau de sécurité informatique.
   La version renforcée du texte aura, en principe, vocation à s'appliquer à plus de 150 000 entreprises, alors que seules quelques centaines d'entre elles étaient jusqu'à présent concernées.
   En outre, le champ d'application du texte serait élargi à de nouveaux secteurs d'activités, tels que la gestion des déchets, la grande distribution, les services postaux, les fournisseurs d'accès à internet, les prestataires de Data center, les secteurs de l'espace et de la recherche ou les entreprises de services numériques.

3. **Caméras augmentées dans les espaces publics**

   La Commission Nationale Informatique et Liberté (CNIL – autorité française de protection des données) s'est récemment prononcée sur l'utilisation des caméras « *augmentées** » dans l'espace public en fixant un cadre à ne pas franchir.
   L'autorité de protection des données a notamment insisté sur les risques existants en termes de droits et de libertés des personnes (risque de surveillance généralisée de l'espace public voire de profilage, etc.), tout en relevant que certains usages pouvaient paraitre légitimes.
   Il convient de rappeler que ces dispositifs permettent, non seulement, de filmer les personnes, mais aussi de déduire, par une analyse d'images, certaines données les concernant.
   La CNIL a, en outre, souligné l'absence de cadre légal permettant d'autoriser l'utilisation de ces dispositifs par la puissance publique en vue de détecter et poursuivre des infractions. En effet, à ce-jour, seule la pose de caméras de vidéosurveillance sur la voie publique est légalement encadrée par le Code de la sécurité intérieure.

   * ***dispositifs constitués de logiciels de traitements automatisés d'images couplés à des caméras***

4. Espace européen de données de santé : avis conjoint du Comité européen de la protection des données et du Contrôleur européen de la protection des données

Le Comité européen de la protection des données (CEPD) et le Contrôleur européen de la protection des données ont rendu, le 12 juillet dernier, un avis conjoint relatif à l'Espace européen des données de santé et à la proposition de règlement.

Ils ont, à cet égard, souhaité attirer l'attention des législateurs sur les points majeurs suivants :

- la localisation, sur le territoire de l'Union européenne, des données de santé entrant dans le champ de la proposition de règlement et ce, en raison de leur sensibilité et du volume que ces dernières représentent (500 millions de citoyens européens) ;
- la nécessaire clarification des interactions entre la proposition de règlement, le RGPD et les législations nationales afin d'assurer une application cohérente des textes, notamment en ce qui concerne les droits des personnes concernées ;
- la compétence exclusive des autorités de protection de données dans le traitement de toute question relative à la protection des données personnelles ;
- la limite des exceptions apportées aux droits des personnes concernées garantis par le RGPD ;
- l'exclusion des données collectées par les applications de bien-être et d'autres applications numériques du champ de la proposition ;
- le respect du principe de la minimisation des données ;
- la délimitation claire des objectifs poursuivis dans le cadre des usages secondaires des données de santé, passant notamment par la démonstration d'un lien suffisant avec des enjeux de protection sociale et de santé publique ;
- la définition d'une articulation cohérente entre les missions du nouveau Comité européen des données de santé et des « *groupes de responsabilité conjointe* ».

En outre, une liste indicative de critères permettant l'identification des cas transfrontaliers stratégiques pour lesquels prioriser des actions de mise en conformité a été arrêtée.

5. Autorités de protection des données et autres Autorités

- Renforcement de la coopération des Autorités de protection européennes

De manière parallèle à l'avis conjoint du CEPD et du Contrôleur européen de la protection des données relatif à l'Espace européen des données de santé, les Autorités de protection des données ont réitérés leur engagement pour une coopération transfrontalière plus étroite et collective.

Sous l'égide du CEPD, elles ont identifié des cas stratégiques appelant une collaboration accrue sur la base des critères suivants :

- Le cas est lié à un problème structurel ou récurrent dans plusieurs États membres, en particulier s'il soulève une question juridique générale relative à l'interprétation, l'application ou la mise en œuvre du règlement général sur la protection des données personnelles (RGPD) ;

- Le cas concerné est situé à l'intersection de la protection des données et d'autres domaines juridiques ;
- Un grand nombre de personnes, dans plusieurs États membres, sont concernées par ce cas ;
- De nombreuses plaintes ont été reçues dans plusieurs États membres en lien avec ce cas ;
- Le cas soulève une question fondamentale relevant de la stratégie du CEPD ;
- Le cas peut entraîner un risque élevé au regard du RGPD, notamment en cas de traitements de données sensibles, des personnes vulnérables (ex. : mineurs) ou, si une analyse d'impact sur la protection des données est requise pour le traitement concerné.

Dans l'hypothèse où un cas viendrait à répondre à un ou plusieurs des critères susvisés, il est prévu la mise en œuvre de deux étapes d'analyse supplémentaires destinées à permettre de confirmer officiellement le caractère stratégique ou non.

- France

Collecte de données de géolocalisation

La société Ubeeqo (intervenant dans le secteur de la location de véhicules pour une courte durée) a été sanctionnée par la CNIL d'une amende de 175.000 euros pour avoir collecté, de manière quasi-permanente, des données de géolocalisation.
L'autorité lui reprochait également une durée de conservation excessive (3 ans à compter de la fin de la location).
A cet égard, elle a eu l'occasion de rappeler que la collecte permanente de données de géolocalisation n'obéit pas au principe de minimisation des données consacré à l'article 5.1 c) du RGPD.
Or, comme elle l'a souligné, la géolocalisation est particulièrement intrusive dans la vie privée des personnes.
La société géolocalisait pourtant les utilisateurs de ses véhicules tous les 500 mètres, lorsque le moteur s'allumait ou s'éteignait ou encore, en cas d'ouverture et de fermeture des portières.
Les justifications avancées par Ubeeqo (maintenance, localisation des véhicules en cas de vol et assistance en cas d'accidents) n'ont pas été jugées suffisantes.
Outre la durée de conservation excessive, la CNIL a relevé des faiblesses au niveau de l'information des personnes concernées, les informations pertinentes n'étant pas suffisamment accessibles par les utilisateurs.

Violation du RGPD – proposition de sanction

Après deux années d'enquête, la CNIL a proposé de sanctionner le spécialiste du reciblage publicitaire sur internet (CRITEO) d'une amende de 60 millions d'euros en raison de plusieurs manquements qui lui seraient imputés, notamment l'absence de base légale pour le traitement de données mis en œuvre.
La société a d'ores et déjà annoncé qu'elle ne manquerait pas de répondre au rapport de la CNIL, tant sur le volet de la violation du RGPD, que sur celui du montant de l'amende proposée.
Une décision définitive devrait être rendue en 2023.

Prospection commerciale sans consentement

Le Groupe ACCOR s'est vu infliger une amende de 600 000 euros en raison de plusieurs infractions au RGPD et une infraction à la législation française. Cette sanction fait suite à des

opérations d'investigations menées après que des plaintes aient été adressées à la CNIL et à plusieurs autres Autorités européennes de protection des données.
Il est notamment reproché au Groupe d'avoir procédé à des opérations de prospection commerciale sans avoir obtenu le consentement préalable des personnes concernées et de ne pas avoir respecté les droits des clients et prospects.
Au cours des investigations menées par la CNIL, il est apparu que les clients étaient automatiquement inscrits à la newsletter lorsqu'une réservation était effectuée sur le site d'un hôtel du groupe ou directement auprès du personnel d'un hôtel. La case était en effet pré-cochée par défaut. En outre, des anomalies techniques ont empêché un nombre significatif de personnes de s'opposer efficacement à la réception des messages de prospection, et ce, pendant plusieurs semaines.

- Grèce

Après les Autorités française et italienne, c'est désormais au tour de l'Autorité hellénique de protection des données de condamner la société américaine Clearview AI à une amende de 20 millions d'euros.
Pour rappel, cette société, spécialisée dans la reconnaissance faciale, a développé un logiciel permettant de rechercher un visage parmi une base de données comportant près de 10 milliards d'images faciales obtenues *via* « *web scarping* » (technique d'extraction de contenus de sites web) et provenant notamment des réseaux sociaux et d'autres ressources en ligne.
Clearview AI est assujettie au RGPD en vertu de son article 3, 2. b)*.
Une fois de plus, il lui est reproché (cette fois par la CNIL grecque) d'utiliser les données personnelles [de grecs] sans leur consentement afin d'alimenter sa base de données dédiée à la reconnaissance faciale.
Partant, la société ne pourra plus utiliser des images de personnes en Grèce. Il lui a de plus été enjoint de supprimer toutes les données personnelles des grecs récoltées jusqu'ici.

****au terme de cet article, le RGPD s'applique au traitement des données relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable de traitement ou un sous-traitant qui n'est pas établi dans l'Union lorsque les activités de traitement sont liées (…) b) au suivi de comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union****.

- Norvège

L'autorité norvégienne de protection des données a sanctionné d'une amende (équivalent à 400.000 euros) l'une des municipalités du pays à qui elle reprochait des manquements en matière de sécurité.
En l'espèce, la municipalité avait été victime d'une cyberattaque qui avait empêché ses employés d'accéder à la plupart des systèmes informatiques.
En outre, un certain nombre de données, en ce compris des informations très sensibles sur les résidents et employés de la municipalité, avaient été cryptées et les sauvegardes effacées.
Après des messages de rançon, une partie des données compromises avaient été publiées sur le « *dark web* ».
L'autorité de protection a ainsi considéré que la sécurité des données personnelles était gravement et fondamentalement défectueuse, notamment s'agissant des journaux, de l'analyse des journaux, de la protection des sauvegardes et de l'absence d'authentification à deux facteurs ou de mesures de sécurité similaires. En outre, le pare-feu était peu configuré en termes de journalisation et une grande partie du trafic interne jamais enregistrée. Enfin, les serveurs n'étaient pas configurés pour envoyer des journaux à un centre de journalisation central et n'enregistraient pas les évènements importants.

- Pologne

Un centre d'aide aux personnes a écopé d'une amende d'un montant équivalent à 2.200 euros pour avoir enregistré, dans ses locaux, des sons et voix à l'aide de son système de surveillance en l'absence de base légale.
Le responsable de traitement a tenté, sans succès, de faire valoir, auprès de l'Autorité polonaise de protection des données, que ce traitement était nécessaire au respect d'une obligation légale.
Selon lui, le système de surveillance lui permettait d'enregistrer, à la fois, des signaux audio et vidéo et ainsi, d'exercer une surveillance continue sur les personnes amenées à dégriser afin d'assurer leur sécurité. Il précisait, en outre, conserver ces éléments de 30 à 60 jours, sauf lorsque l'enregistrement servait de preuve dans une procédure en cours.
L'Autorité de protection des données a considéré que l'enregistrement des voix des personnes était excessif et que le centre ne pouvait, par ailleurs, pas évoquer l'un des motifs énumérés à l'article 6.1 du RGPD relatif à la licéité. Cela étant, pour fixer le montant de l'amende, l'autorité a retenu que le responsable de traitement avait cessé, dès le début de l'ouverture de la procédure administrative, le traitement de données et effacé les données enregistrées.

Autres Autorités

- **Conseil Constitutionnel français : précisions apportées sur le sort des données de connexion dans le cadre d'instructions préparatoires**

Le Conseil Constitutionnel a apporté des précisions sur les articles 99-3 et 99-4 du code de procédure pénale dans leur rédaction résultant de la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement et améliorant l'efficacité et les garanties de la procédure pénale.
Il était reproché à ces deux dispositions de permettre au juge d'instruction ou à l'officier de police judiciaire (OPJ) commis par ce dernier de pouvoir requérir la communication de données de connexion alors qu'une instruction peut porter sur tout type d'infraction et n'est ni justifiée par l'urgence ni limitée dans le temps, ce qui porterait une atteinte au droit au respect de la vie privée.
La Haute Juridiction a pourtant écarté ce grief.
Elle a notamment jugé que :

- La réquisition de données de connexion intervient à l'initiative du juge d'instruction, magistrat du siège dont l'indépendance est garantie par la Constitution ou, par l'OPJ autorisé par une commission rogatoire délivrée par ce magistrat ;
- Ces deux articles ne permettent la réquisition de données de connexion que dans le cadre d'une information judiciaire dont l'ouverture n'est obligatoire, qu'en matière criminelle ou pour certains délits. Dans les autres cas, le juge d'instruction ne peut informer qu'en vertu d'une réquisition du procureur de la République ou à la suite d'une plainte avec constitution de partie civile (dans les conditions prévues à l'article 85 du code de procédure pénale) ;
- Dans les cas où la réquisition de données de connexion est mise en œuvre par un OPJ en exécution d'une commission rogatoire, celle-ci est datée et signée par le magistrat. Il y est, en outre, précisé la nature de l'infraction, l'objet des poursuites. De même, un délai dans lequel elle doit être retournée avec les procès-verbaux dressés par les OPJ pour son exécution. Ces réquisitions doivent se rattacher directement à la répression de l'infraction et sont mises en œuvre sous la direction et le contrôle du juge d'instruction ;
- Enfin, la durée de l'information ne doit pas, sous le contrôle de la chambre de l'instruction, excéder un délai raisonnable au regard de la gravité des faits reprochés à

la personne mise en examen, de la complexité des investigations nécessaires à la manifestation de la vérité et de l'exercice des droits de la défense.
Cons. const. 17 juin, n° 2022-1000 QPC

- **Cour de Justice de l'Union Européenne (CJUE) : traitement des données des passagers aériens**

Au terme d'un arrêt rendu le 21 juin 2022, la CJUE s'est prononcée en faveur d'une limitation des pouvoirs prévus par la Directive européenne sur les données des dossiers passagers (directive 2016/681 PNR (Passager Name Record) du 27 avril 2016).
Au terme de cette Directive, il est introduit un mécanisme en vertu duquel les compagnies aériennes collectent et transfèrent, aux Autorités répressives nationales, les données des passagers aériens (Données PNR) provenant de vols extra-UE dans le but de prévenir, détecter ou enquêter sur les activités terroristes et les crimes graves. Sont notamment concernées les données relatives au nom du passager, aux dates de voyage, à l'itinéraire, au numéro de siège, aux bagages, aux modes de paiement, etc.
En vertu de l'article 2, les Etats Membres (EM) peuvent étendre ces procédures de contrôle aux vols *intra-UE* à condition d'en informer la Commission européenne.
A l'exception de l'Autriche et de l'Irlande, les EM ont déclaré qu'ils procéderaient à cette déclaration.

En 2017, La ligue des droits de l'homme a introduit un recours en annulation à l'encontre de la loi belge de transposition (Loi du 25 décembre 2016), devant la Cour Constitutionnel belge. Il lui était reproché d'introduire une surveillance généralisée portant atteinte aux droits fondamentaux à la vie privée et à la protection des données. L'association contestait, par ailleurs, le fait que la directive PNR aille à l'encontre du principe fondamental de libre circulation des personnes arguant que les contrôles des vols *intra-UE* rétablissaient *de facto* un contrôle aux frontières.

L'affaire a dès lors été renvoyée devant la CJUE, étant précisé que pas moins de 10 questions préjudicielles lui ont été posées, certaines portant notamment sur la validité de la Directive PNR et sur la compatibilité de la loi belge de transposition avec le droit de l'Union.
Si la CJUE n'est pas allée jusqu'à abroger l'ensemble de la législation, comme l'aurait souhaité la Ligue des droits humains, elle a cependant reconnu que la directive PNR comportait des ingérences d'une gravité certaine en termes d'atteinte aux droits à la vie privée et à la protection des données en introduisant notamment un mécanisme de surveillance continue, non ciblée et systématique.
Partant, elle a jugé qu'« *[E]n l'absence de menace terroriste réelle et actuelle ou prévisible à laquelle fait face un État membre, le droit de l'Union s'oppose à une législation nationale prévoyant le transfert et le traitement des données PNR des vols intra-UE ainsi que des transports effectués par d'autres moyens à l'intérieur de l'Union* ».
Elle a également interprété strictement le pouvoir conféré par la directive aux Autorités publiques, ordonnant notamment que ces traitements et conservation des données soient limités à ce qui est strictement nécessaire pour lutter contre le terrorisme et la criminalité grave et s'opposant à une conservation généralisée des données (de 5 ans) applicable indifféremment à tous les passagers aériens.