ACTUALITÉS OCTOBRE 2021

1. G7 des autorités de protection des données

Une première édition du G7 de la protection des données a eu lieu, les 7 et 8 septembre 2021, au Royaume-Uni.
Cette réunion, qui regroupe les autorités de protection des données des pays membres du G7, succède à celle qui a réuni, en avril 2021, les ministres du numérique et des technologies.
Les autorités de protection des données française, canadienne, allemande, italienne, japonaise, britannique et américaine ont, à cette occasion, échangé sur de nombreux sujets, parmi lesquels l'intelligence artificielle et la protection des données, la protection des données et le droit de la concurrence, la circulation des données à l'échelle internationale, l'élaboration d'un cadre pour le transfert transfrontalier des données et la coopération des autorités de contrôle.
Une nouvelle réunion est prévue en 2022.

2. Royaume-Uni et loi sur la protection des données

Le Ministère du Numérique, des médias, de la culture et des sports a récemment publié une consultation sur la future loi britannique relative à la protection des données personnelles.

Celle-ci propose des modifications de la loi actuelle, dont certaines sont substantielles et porteraient sur les droits des personnes concernées, l'« *accountability* », les transferts de données, la protection de la vie privée en ligne.

Cette consultation est ouverte jusqu'au 19 novembre prochain.

3. Arrêts de la CEDH

➢ Droit au respect de la vie privée et droit de la preuve

Production de messages électroniques privés devant les juridictions civiles (***CEDH, 7 sept. 2021, MP c/ Portugal***)

En l'espèce, des messages électroniques, échangés sur un site de rencontre, avaient été produits par un mari, dans le cadre d'une procédure de divorce, afin d'apporter des preuves de relations extra-conjugales de son épouse.
Cette dernière a déposé une plainte contre son mari pour violation du secret des correspondances, laquelle a abouti à un non-lieu.
Une requête a donc été introduite, devant la CEDH, sur le fondement de l'article 8 de la Convention européenne des droits de l'homme consacrant le droit au respect de la vie privée (dont fait partie le secret des correspondances).
En l'espèce, la CEDH a opéré un contrôle de proportionnalité entre le droit au secret des correspondances et le droit de la preuve.
Elle finit par retenir qu'aucune violation de l'article 8 de la Convention ne peut être imputée à l'époux et considère que « *les effets de la divulgation des messages litigieux sur la vie privée de la requérante ont été limités* » puisque « *ces messages n'ont été divulgués que dans le cadre des procédures civiles. Or, l'accès du public aux dossiers de ce type de procédures est restreint. De plus, les messages n'ont pas été examinés concrètement, le tribunal aux affaires familiales n'ayant pas statué sur le fond des demandes formulées par le mari* ».

4. Avis du Comité Européen à la Protection des Données

Le Comité Européen à la Protection des Données (CEPD) remplace l'ancien Groupe 29 et a vocation à veiller au respect du RGPD. Il peut être saisi par les autorités de protection des données européennes.

➢ Procédure d'adéquation de la Corée du sud et Union Européenne

Des discussions sont menées depuis 2017 entre l'Union Européenne et la Corée du Sud pour parvenir à une décision d'adéquation, qui faciliterait le transfert de données UE/Corée du Sud.
Le CEPD a récemment rendu un avis, non-contraignant, sur le projet d'adéquation de la Commission Européenne pour la République de Corée.
Dans le cadre de ce dernier, il a considéré que le cadre de protection des données sud-coréen était, en grande partie, aligné sur celui de l'Union Européenne s'agissant des concepts clés de :

- Finalité et justification du traitement ;
- Limitation de traitement ;
- Durée de conservation, sécurité et confidentialité ;
- Transparence.

Quelques réserves ont toutefois été émises notamment concernant les exemptions relatives à la sécurité nationale.
En effet, la Corée du sud ne limite pas l'accès aux données personnelles par les forces de l'ordre.
Il en est de même en termes de pseudonymisation des données, de la possibilité limitée de retirer, à tout moment, son consentement, de la définition de la notion de « *sous-traitant* », du manque de protection par rapport à la prise de décision automatisée.
Le CEPD a enfin demandé à la Commission européenne de surveiller toute évolution susceptible d'entraver l'indépendance de l'autorité de protection des données sud-coréenne.

Pour rappel, la Corée du sud ne figure pas sur la liste des pays disposant d'un niveau de protection adéquat au sens de l'article 20 de la Loi monégasque n° 1.165 du 23 décembre 1993, modifiée.

5. Utilisation de la reconnaissance faciale par la police et adoption d'une résolution en faveur d'un moratoire par les députés de l'Union européenne

Les eurodéputés ont adopté, le 6 octobre dernier, (par 377 voix contre 248 et 62 abstentions) une résolution pour demander un moratoire sur le déploiement des systèmes de reconnaissance faciale par les forces de l'ordre afin de garantir le droit à la vie privée.
Ils ont souligné « *le risque de biais algorithmiques dans les applications d'intelligence artificielle (IA)* » et ont précisé « *que des contrôles humains et juridiques élevés sont nécessaires pour prévenir la discrimination par l'IA, en particulier dans le cadre des services répressifs ou dans un contexte transfrontalier. Les décisions finales doivent toujours être prises par un être humain et les personnes soumises à des systèmes alimentés par l'IA doivent disposer de voies de recours* ».
L'interdiction permanente de la reconnaissance automatisée des individus dans les espaces publics a également été demandée, sauf en cas de soupçons d'un crime.
Les eurodéputés ont enfin demandé aux États membres de faire savoir si leurs services répressifs utilisent des outils d'identification de type Clearview (*cf. : point 6. Autorités de contrôle – Finlande*) et ont exprimé leur volonté d'interdire les systèmes de notation sociale.

La résolution est disponible ici.

6. Géolocalisation et vie privée

Le Conseil constitutionnel français s'est récemment prononcé sur une question prioritaire de constitutionnalité (*QPC*) relative à la conformité, aux droits et libertés garantis par la Constitution, des articles 230-21 et 230-33 du Code de procédure pénale français (relatifs à la géolocalisation) dans leur rédaction résultant de la loi du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice (*Cons. Const., 23 sept. 2021, n° 2021-930 QPC*).

Il était reproché à ces dispositions de permettre, au procureur de la République, d'autoriser, sans contrôle préalable d'une juridiction indépendante, le recours à une opération de géolocalisation dans le cadre d'une enquête qu'il dirige.

En effet, s'agissant d'enquêtes de flagrance ou préliminaire ou d'une procédure prévue aux articles 74 et 74-2 du code de procédure pénale, la géolocalisation peut être autorisée par le procureur de la République.

Aux termes d'une décision rendue le 23 septembre 2021, le Conseil Constitutionnel a considéré que « *les dispositions contestées, qui ne sont pas entachées d'incompétence négatives et qui ne méconnaissent pas non plus les droits de la défense et le droit à un recours juridictionnel effectif, ni aucun autre droit ou liberté que la Constitution garantit, doivent être déclarées conformes à la Constitution* ».

Plus particulièrement, il a :

- Relevé que la surveillance par le biais d'une géolocalisation n'implique ni acte de contrainte sur la personne visée, ni atteinte à son intégrité, de saisie, interception de correspondance ou enregistrement d'image ou de son ;

- Estimé que les mesures de géolocalisation étaient entourées de garanties permettant d'assurer une conciliation équilibrée entre l'objectif de valeur constitutionnelle de recherche des auteurs d'infractions et le droit au respect de la vie privée.

7. Autorités de contrôle européennes

➢ France

- Lancement d'une consultation publique sur un projet de guide ayant vocation à aider les professionnels du recrutement à respecter la protection des données. Cette consultation est ouverte jusqu'au 19 novembre 2021.

- Publication d'un livre blanc sur les données et moyens de paiement intitulé « *Quand la confiance paie* ».

- La CNIL a récemment rappelé à l'ordre le Ministère de l'Intérieur en raison de sa mauvaise gestion du fichier automatisé des empreintes digitales.
  Ce fichier de police recense les empreintes digitales de personnes mises en cause dans des procédures pénales, ainsi que les traces d'empreintes relevées sur les scènes de crimes et de délits. Il est géré par le Ministère de l'Intérieur et est utilisé par les services de police, de gendarmerie et par les douanes. Il contient des empreintes digitales et palmaires relevées sur des personnes ainsi que certaines informations les concernant (nom, prénom, filiation, sexe, date et lieu de naissance) et relatives au contexte de la collecte (date et lieu d'établissement

de la fiche, nature de l'affaire, etc.). Il recense également les traces relevées sur le lieu de commission d'une infraction.

Divers manquements ont motivé le rappel à l'ordre de la CNIL, parmi lesquels :

- La conservation de données non prévues par les textes (ex. le nom de la victime enregistré dans les fiches « traces » sous forme d'image rendant toute recherche impossible),
- La conservation de données pendant une durée supérieure à celle prévue par les textes et, qui plus est, relatives à des personnes ayant bénéficié d'un acquittement, d'une relaxe, d'un non-lieu ou d'un classement sans suite (sur ce point la formation restreinte de la CNIL a relevé que « *les décisions de relaxe, d'acquittements, de non-lieu et de classement sans suite sont rendues par les autorités judiciaires et qu'elles doivent ensuite être transmises au service du gestionnaire du FAED à l'aide de fiches navettes afin que les décisions soient répercutées et que soient effacées les données devant l'être* ») ;
- L'utilisation de mots de passe peu robustes entrainant une sécurité insuffisante des données ;
- L'absence d'informations des personnes concernées (pas d'affichage dans les locaux de garde à vue, pas d'information au moment où la décision est prononcée ou signifiée, ni à un autre moment, sous réserve des restrictions prévues par le décret instaurant le traitement).

Partant, la CNIL a demandé :

- La suppression des fiches d'un ancien fichier manuel qui aurait déjà dû être supprimé ;
- L'effacement de données dont la collecte n'a pas été prévue par le décret relatif au fichier automatisé des empreintes digitales ;
- La suppression des fichiers dont la durée de conservation est atteinte ;
- Qu'il soit assuré que les décisions de relaxe, d'acquittement et de correctionnalisation soient répercutées dans le fichier ;
- Qu'il soit assuré que les décisions de non-lieu et de classement sans suite soient répercutées dans le fichier automatisé des empreintes digitales uniquement en cas de demande expresse du procureur de la République ;
- Le renforcement de la sécurité de la connexion au fichier ;
- La délivrance d'une information aux personnes dont les empreintes sont versées au fichier automatisé des empreintes digitales.

Une mise en conformité doit être effectuée au 31 octobre 2021 avec une possible prorogation du délai expirant le 31 décembre 2022.

- **Irlande**

Le CEPD a demandé à l'autorité irlandaise de modifier son projet de décision de sanction à l'égard de WhatsApp.

Les 21 mai et 20 août 2020, les décisions préliminaires de l'autorité irlandaise avaient été notifiées à WhatsApp.
Ces dernières, qui avaient été communiquées aux autres autorités européennes, n'avaient toutefois pas fait l'unanimité. Faute d'accord entre elles, l'autorité irlandaise a donc activé le

mécanisme prévu par l'article 65 du RGPD (*ce mécanisme prévoit une possible saisine du CEPD par une autorité de contrôle en vue d'assurer l'application cohérente et conforme du règlement*).

Dans un avis contraignant rendu le 23 avril 2021, la CEPD a estimé que WhatsApp avait bien accès à des données de non-utilisateurs. Il a été également souligné les atteintes au principe de transparence par WhatsApp.
En outre, il a été demandé à l'autorité irlandaise des précisions concernant le calcul de la sanction. Le CEPD a, à cet égard, précisé les contours de l'article 83 paragraphe 3 du RGPD (*conditions générales pour l'imposition d'amendes administratives*) en rappelant que les autorités de contrôle doivent tenir compte du chiffre d'affaires de l'ensemble des sociétés du groupe et que ce dernier devait être retenu pour déterminer le montant maximal de l'amende envisagée, l'ensemble des défauts de conformité devant, par ailleurs, être pris en compte.

- **Finlande**

- Le 20 septembre dernier, l'autorité de protection des données finlandaise a rappelé à l'ordre le Conseil national de la police (CNP) à propos de l'usage d'un procédé de reconnaissance faciale *via* le logiciel Clearview AI.
En avril 2021, la CNP avait porté à la connaissance de l'autorité de protection l'existence d'une fuite de données en lien avec l'utilisation expérimentale de ce logiciel.
Précisons que ce traitement avait été mis en œuvre, sans l'autorisation préalable de l'autorité de protection des données.
Outre le rappel à l'ordre, il a ainsi été enjoint, au Conseil national de police, de contacter l'ensemble des personnes concernées par cette fuite (dans la mesure où leur identité peut être déterminée) et demander à Clearview d'effacer, de ses plateformes de stockage, toutes les données transmises par la police.

- Un blâme a été prononcé, à l'encontre d'une société finlandaise, sur le fondement des articles 14 (*informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée*) et 15 (*droit d'accès de la personne concernée*) du RGPD.
Une plainte avait été transmise à l'autorité de contrôle après qu'un ancien membre d'un conseil d'administration ait découvert que son entreprise avait accédé à sa messagerie professionnelle. L'autorité a, en l'espèce, conclu que si l'entreprise avait bien une base juridique pour lui permettre d'accéder audit compte, elle n'avait pas suffisamment informé le plaignant quant à ce possible accès.
Elle a, en outre, estimé que l'entreprise avait attendu trop longtemps pour répondre à la demande de droit d'accès adressée par le plaignant.
Enfin, l'autorité a ordonné que des procédures écrites soient mises en place pour permettre l'accès aux comptes de messagerie.

- **Royaume-Uni**

- Plusieurs écoles britanniques ont récemment introduit un système de reconnaissance faciale afin de faciliter le paiement des frais de cantine par les élèves. Ainsi, le visage de chaque élève est scanné dans la file d'attente.
À cet égard, l'autorité de protection des données britannique s'est inquiétée de cette pratique et a rappelé que ces établissements doivent se conformer aux règles applicables en matière de protection des données personnelles (des règles particulières existant pour les mineurs). Elle les a également invités à adopter une approche moins intrusive.

8. Monde numérique

Europe

- France

❖ **Office 365 et État français**

La Direction interministérielle du numérique a adressé à l'Agence nationale de la sécurité des systèmes d'informations (*ANSSI – A Monaco, l'équivalent est l'Agence Monégasque de Sécurité Numérique – AMSN*) et aux directions des systèmes d'information des différents ministères une note leur indiquant qu'Office 365 n'était plus conforme avec la doctrine Cloud de la DSI de l'État français.

Celle-ci prévoit notamment, qu'en cas de système numérique manipulant des données sensibles, le cloud auquel il est recouru doit être immunisé contre les règlementations extracommunautaires.

Les DSI des ministères sont donc invitées à ne plus utiliser ou ne pas installer Microsoft Office 365 avec quelques dérogations pour une durée de 12 mois.

Pour répondre à cette interdiction, une plateforme de communication souveraine destinée à l'administration publique vient d'être déployée entre OVHcloud et Whaller. Pour rappel, le cloud privé d'OVH est qualifié SecNUMcloud par l'ANSSI (ce qui garantit un très haut niveau de sécurité).

❖ **Alliance Thalès et Google Cloud**

Un projet de label français « *Cloud de confiance* » a été lancé au mois de mai dernier, entre la société Thalès et Google Cloud.

L'objectif annoncé est de concilier souveraineté numérique et compétitivité économique.

Des inquiétudes ont été relayées par les acteurs du cloud français notamment celle qu'un « *grand acteur américain prenne position sur le marché français, pourtant souhaité comme un marché du « cloud souverain »* ».