ACTUALITÉS MARS 2022

1. **Encadrement des transferts de données Europe/Etats-Unis**

   Suite à l'invalidation du Privacy Shield, par la Cour de justice de l'Union européenne, en juillet 2020, un accord de principe aurait finalement été trouvé entre les Etats-Unis et l'Union européenne. Les détails techniques et juridiques de ce dernier doivent cependant encore être arrêtés. Cet accord fait en effet suite à la transmission d'une offre par les Etats-Unis, en février dernier, laquelle prévoirait notamment la création d'une agence agissant sous la direction du département de justice américaine et qui serait chargée de surveiller le traitement des données européennes par les services de renseignement américains.

   Affaire à suivre d'autant qu'une décision de la Cour Suprême des Etats-Unis (*FBI c/ Faraganza*) a récemment accordé plus de latitudes au Gouvernement américain pour invoquer le secret d'Etat dans les affaires d'espionnage.

2. **Règlementation Britannique relative au transfert de données personnelles hors du Royaume-Uni**

   Dans le prolongement du Brexit et de l'adoption du *UK Data Protection Act 2018*, l'encadrement des transferts de données au départ du Royaume-Uni a fait l'objet d'une évolution récente.

   En effet, ces transferts seront désormais régis par le nouvel accord international sur les transferts de données (*International Data Transfer Agreement - IDTA*), le nouvel Addendum sur le transfert international de données aux nouvelles clauses contractuelles types de l'Union européenne (UE) (*UK Addendum*) ainsi par des dispositions transitoires, notamment pour les contrats conclus avant le 21 septembre 2021 sur la base des clauses contractuelles types de l'UE.

   La signature de l'un de ces documents servira d'outil de transfert de données.

   Rappelons que jusqu'à présent, les transferts de données hors du Royaume-Uni, vers des pays considérés comme ne disposant pas d'un niveau de protection adéquat étaient conditionnés à la mise en œuvre de garanties appropriées, ce qui impliquaient, en amont, la réalisation d'évaluations de risques liés au transfert.

   De même, il était prévu la signature de clauses contractuelles types pour les autres transferts de données.

   Notons que s'agissant de l'*IDTA*, ce dernier ne pourra être utilisé que pour les transferts de données soumis aux Lois britanniques de protection des données et non à ceux soumis au RGPD.

   Pour ce qui est du *UK Addendum*, celui-ci permettra aux organisations, à la fois soumises aux Lois britanniques et au RGPD, d'effectuer des transferts de données, sans nécessité de conclure d'accord distinct concernant le Royaume-Uni.

3. **Effacement de données indûment transférées aux Etats-Unis**

   A l'effet d'un jugement en date du 7 novembre 2022, le Tribunal judiciaire de Grenoble a ordonné à la Banque Rhône-Alpes de « *faire toutes les diligences à ses frais auprès des autorités fiscales des Etats-Unis pour qu'elles procèdent à l'effacement total de ses déclarations FATCA antérieurs à 2017 impliquant à tort son client* ».

   Le FATCA [Foreign Account Tax Compliance] est un règlement en vertu duquel les institutions financières non-américaines doivent communiquer au fisc américain toute information pertinente au sujet de comptes financiers détenus par un client identifié comme étant un contribuable américain.

En l'espèce, le lieu de naissance du client avait fait l'objet d'une erreur, celui-ci étant né à Ottawa capitale canadienne et non à Ottawa, nom d'une ville des Etats-Unis. En dépit des demandes de corrections du client, la Banque avait maintenu son erreur considérant que ce dernier ne justifiait pas ne pas être né aux Etats-Unis. Elle avait donc poursuivi ses déclarations outre-Atlantique.
A la suite de la fourniture d'un acte de naissance, la banque s'était finalement exécutée, mais uniquement pour l'année 2017. En outre, elle n'avait pas communiqué l'existence de l'erreur de lieu de naissance aux autorités américaines, de sorte que si l'inscription du client sur la liste des personnes concernées a bien été modifiée, elle n'a cependant pas été effacée.
Aussi, se fondant sur l'article 17 du Règlement européen pour la protection des données, le tribunal judiciaire de Grenoble a notamment retenu que « *la banque, professionnelle du droit et particulièrement tenue à ce titre d'un devoir de vigilance,* ***ne pouvait ignorer que le droit à l'effacement est un droit reconnu tant par la législation française que par les textes et la jurisprudence européennes et ne pouvait ignorer les contraintes particulières attachées d'une part à la transmission de données vers un Etat n'appartenant pas à l'Union Européenne et d'autre part à l'exercice du droit d'effacement pour les traitements mis en œuvre par les administrations publiques****. ».*
La condamnation de la banque, a été assortie d'une astreinte de 1.500 euros par jour de retard et de l'exécution provisoire.

4. Identification du directeur de la publication d'un compte Facebook

Par jugement correctionnel du 3 janvier 2022, le Tribunal judiciaire de Fontainebleau a jugé qu'un numéro de téléphone utilisé pour la création d'un compte Facebook est un élément suffisant pour établir que le titulaire dudit numéro dispose de la qualité de directeur de publication du compte.
Ce dernier a ainsi fait l'objet d'une condamnation en raison de la publication de propos diffamatoires à l'encontre d'un maire.

5. Europol – prérogatives en matière de données personnelles

Le Contrôleur européen à la protection des données (CEPD) (autorité indépendante de l'Union européenne chargée de la protection des données) a sommé, en début d'année, Europol (Agence européenne de police criminelle) de supprimer, dans un délai de 12 mois, un certain nombre de données (celles transmises par les pays membres de l'UE sur des individus soupçonnés d'activité criminelle qui n'auraient pas été filtrées par Europol depuis plus de 6 mois).
Le CEPD reprochait à l'Agence un manquement au principe de minimisation des données et aux règles de durée de conservation. Un premier avertissement lui avait d'ailleurs été adressé en ce sens dès 2020, sans que celui-ci n'ait été suivi d'effet.

En pratique, cette demande de suppression ne devrait toutefois pas aboutir. Le 1er février dernier, la Présidence du Conseil de l'Union européenne et le Parlement se sont accordés sur un projet de règlement destiné à modifier le règlement 2016/94 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs.
La coopération d'Europol, dans le cadre de son nouveau mandat, devrait être étendue et lui permettre :

- de recevoir des données à caractère personnel d'entités ou de personnes privées, dans le respect d'exigences strictes en matière de protection de ces données ;
- d'échanger des données personnelles avec des pays tiers, si ces derniers répondent bien aux exigences de garanties appropriées ;

En outre, parmi ses prérogatives, elle devrait collaborer et soutenir les enquêtes du Parquet européen en lui donnant des accès aux données qu'elle détient dans le respect des garanties applicables.
Par ailleurs, en termes de conservation des données, Europol aura 3 ans pour procéder à l'analyse préalable des données et catégoriser les personnes identifiées. S'agissant des données, d'ores et déjà en sa possession, il est prévu que les Etats membres de l'Union européenne, le Parquet européen et l'unité de coopération judiciaire Eurojust n'auront simplement qu'à l'informer qu'ils souhaitent que le nouveau mandat leur soit appliqué.
Il est également prévu qu'Europol puisse proposer aux Etats membres l'introduction de signalements reçus de pays hors UE ou d'organisations internationales dans le système d'information Schengen et qui prendraient la forme d'alertes accessibles uniquement aux policiers situés aux zones Schengen et frontières de l'UE.

6. Données de connexion et censure du Conseil constitutionnel

A titre liminaire, il convient d'indiquer que l'article 34-1 du code des postes et des communications électroniques français encadre le traitement des données à caractère personnel dans le cadre de la fourniture au public de services de communications électroniques.

En décembre dernier, le Conseil constitutionnel du pays voisin avait été saisi d'une Question Prioritaire de Constitutionnalité relative à la conformité des paragraphes II et III de cet article, dans leur rédaction issue de la Loi n° 2013-1168 du 18 décembre 2013 (intitulée *Loi relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale*) aux droits et libertés que la Constitution garantit.

Au titre du paragraphe II de l'article susvisé, les opérateurs de communications électroniques étaient censés effacer ou anonymiser les données relatives au trafic enregistrées à l'occasion des communications électroniques dont ils assurent la transmission.
Les données relatives au trafic sont des données traitées en vue de l'acheminement d'une communication, par un réseau de communications électroniques, ou d'une facturation – *ex. informations permettant d'identifier l'utilisateur, données relatives aux équipements terminaux de communication utilisés, mais également données permettant d'identifier le/les destinataires, etc.*

Le paragraphe III de ce même article, dans sa rédaction issue de la Loi n° 2013-1168, prévoyait que les opérateurs puissent être tenus de conserver certaines catégories de données de connexion, parmi lesquelles les données de trafic (*informations techniques générées par l'utilisation des réseaux de communications – ex. : les adresses IP de l'ordinateur utilisé, la date, l'heure, la durée de chaque connexion, le numéro de téléphone appelé*) en vue de leur mise à disposition de l'autorité judiciaire pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales.

Dans le cadre de la QPC soumise au Conseil Constitutionnel, les requérants reprochaient à ces dispositions d'imposer, aux opérateurs de communications électroniques, une conservation générale et indifférenciée des données de connexion, sans que celle-ci ne soit réservée aux infractions les plus graves, ni conditionnée à l'autorisation ou au contrôle d'une juridiction ou d'une autorité indépendante. Ils dénonçaient de ce fait une atteinte disproportionnée au droit au respect de la vie privée.

Par décision du 25 février 2022, le Conseil constitutionnel a soulevé qu'en « [*E*]*n vertu de l'article 34 de la Constitution, il appartient au législateur de fixer les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques. Il lui incombe*

d'assurer la conciliation entre, d'une part, les objectifs de valeur constitutionnelle de sauvegarde de l'ordre public et de recherche des auteurs d'infractions et, d'autre part, le droit au respect de la vie privée ».

Il a ainsi jugé qu' « *en adoptant les dispositions contestées, le législateur a poursuivi les objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions* » en constatant cependant que « *les données de connexion (…) portent non seulement sur l'identification des utilisateurs des services de communications électroniques, mais aussi sur la localisation de leurs équipements terminaux de communication, les caractéristiques techniques, la date, l'horaire et la durée des communications ainsi que les données d'identification de leurs destinataires**. Compte tenu de leur nature, de leur diversité et des traitements dont elles peuvent faire l'objet, ces données fournissent sur ces utilisateurs ainsi que, le cas échéant, sur des tiers, des informations nombreuses et précises, particulièrement attentatoires à leur vie privée** ».

Cette conservation générale (en ce qu'elle concernait tous les utilisateurs de services de communications électroniques et portait indifféremment sur toutes les données de connexion des personnes, sans tenir compte de leur sensibilité ou de la nature et la gravité des infractions susceptibles d'être recherchées) portait donc une atteinte disproportionnée à la vie privée.

Le Conseil constitutionnel a néanmoins relevé que ces dispositions n'étaient plus en vigueur (la Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement est en effet venue modifier l'article 34-1 du code des postes et des communications électroniques).

Aussi, le Conseil Constitutionnel a finalement jugé que « *la remise en cause des mesures ayant été prises sur le fondement de ces dispositions méconnaîtrait les objectifs de valeur constitutionnelle de sauvegarde de l'ordre public et de recherche des auteurs d'infractions et aurait ainsi des conséquences manifestement excessives* » jugeant que « *ces mesures ne peuvent être contestées sur le fondement de cette inconstitutionnalité* ».
Cons. Const. 25 févr. 2022, n° 2021-967/977 QPC

7. Création d'un traitement automatisé des données pour l'accès aux origines

Par Décret n° 2022-360 du 14 mars 2022, un traitement automatisé de données « *Origines personnelles - ORPER* » a été créé afin de permettre l'accès aux origines personnelles des personnes nées avec une demande de secret de l'identité du parent de naissance.
Le Décret est disponible ICI.

8. Enquêtes et sanctions prononcées par les autorités de contrôle et juridictions européennes

➢ Irlande

- ***META***

  L'Autorité de protection irlandaise (DPC) a sanctionné META (anciennement Facebook) d'une amende de 17 millions d'euros en raison d'une série de violations de données utilisateurs sur plusieurs années. Une enquête avait été ouverte à la suite de notifications de violations de données par META entre le 7 juin 2018 et le 4 décembre 2018.
  Au terme de son enquête, la DPC a constaté une absence de mesures techniques et organisationnelles appropriées, sans pour autant donner des précisions sur la nature des violations constatées.

- ***DPC***

  L'Autorité de protection irlandaise est par ailleurs poursuivie devant la Haute Cour irlandaise par le Conseil Irlandais pour les libertés civiles. Cette poursuite fait suite à la plainte qui avait été déposée par l'un de ses membres contre les technologies publicitaires de Google et de l'IAB et, plus précisément, contre la méthode de ciblage personnalisé des publicités en ligne dont le fonctionnement mobiliserait des données personnelles sans autorisation des personnes concernées. Une enquête avait été ouverte par l'Autorité de protection irlandaise en 2019.

  Or, le membre de l'association reprochait notamment à l'Autorité d'avoir écarté le volet sécurité des données de son enquête et de ne pas avoir traité sa requête dans un délai raisonnable.

  Affaire à suivre, d'autant qu'une plainte pour corruption a, par le passé, été déposée à l'encontre de cette même autorité par Max SCHREMS.

➢ **Pologne**

L'autorité de protection des données polonaise a sanctionné d'une amende de 1.080.000 euros la société Fortum Marketing and Sales Polska SA en raison de divers manquements au RGPD liés notamment à l'absence de mise en place de mesures techniques et organisationnelles.

Le sous-traitant de la société a quant à lui écopé d'une amende de 55.000 euros.

➢ **Italie**

Dans le prolongement de la mise en demeure prononcée, en décembre dernier, par la CNIL, l'Autorité de protection des données italienne (*Garante per la protezione dei dati personali*) a infligé, à la société CLEARVIEW AI, une amende de 20 millions d'euros pour violation du RGPD et l'a sommée de supprimer les données détenues sur des italiens. En outre, tout traitement de reconnaissance faciale dans le pays lui a été interdit.

Pour rappel, CLEARVIEW AI a développé un logiciel de reconnaissance faciale et a constitué une base de données en « aspirant » des photographies et des vidéos publiquement accessibles sur internet.

L'Autorité de protection des données italienne a ainsi constaté plusieurs atteintes portant notamment sur :

- l'obligation de transparence, les personnes n'étant pas suffisamment informées de l'utilisation de leurs images ;
- la finalité du traitement ;
- l'atteinte à la conservation des données sans limite de stockage.