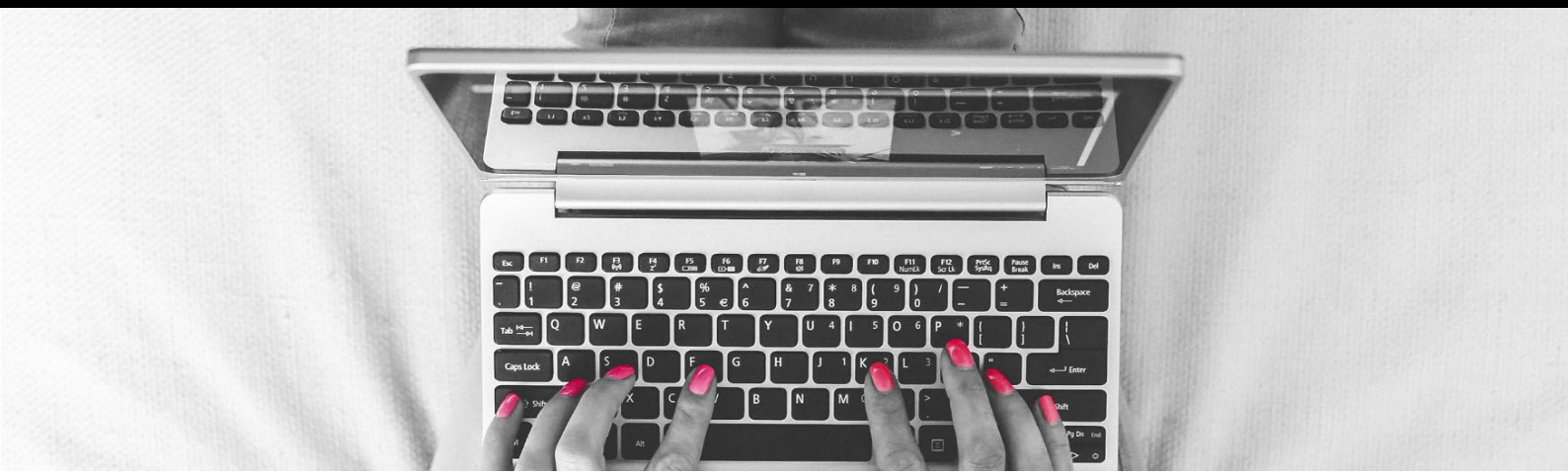
NEWSLETTER DPO

J&A
JOFFE & ASSOCIÉS



1) SANCTION CNIL : LA SOCIÉTÉ SAF LOGISTICS CONDAMNEE A 200 000 EUROS D'AMENDE

Le 18 septembre 2023, la Commission Nationale de l'Informatique et des Libertés (CNIL) a sanctionné la société de fret aérien chinoise SAF LOGISITIC d'une amende de 200 000 euros et a publié la sanction sur son site internet.

La sévérité de cette sanction se justifie par la gravité des manquements commis par la société :

- **Non-respect du principe de minimisation** (**article 5-1 c du RGPD**) : le responsable de traitement ne doit en effet collecter que les seules données nécessaires à la finalité du traitement. Or, en l'espèce, la société collectait des données personnelles des membres de la famille des salariés (identité, coordonnées, fonction, employeur et situation maritale) qui n'avaient aucune utilité apparente.

- **Collecte illicite de données sensibles (article 9 du RGPD) et de données relatives aux infractions, aux condamnations et aux mesures de sûreté (article 10)** : il était en l'espèce demandé à des salariés de renseigner des données dites sensibles, à savoir le groupe sanguin, l'appartenance ethnique et l'affiliation politique. Or, par principe, la collecte de données sensibles est interdite. Elle est permise par exception, si elle apparaît légitime au regard de la finalité du traitement et que le responsable de traitement dispose d'une base légale adaptée, ce qui n'était pas le cas en l'espèce. Par ailleurs, SAF LOGISITIC collectait et conservait des extraits de casiers judiciaires de salariés travaillant dans le fret aérien, faisant déjà l'objet d'une habilitation par les autorités compétentes après enquête administrative. Ainsi, une telle collecte n'apparaissait pas nécessaire.

- **Absence de coopération avec l'autorité de contrôle (article 31 du RGPD) :** La CNIL a en outre considéré que la société avait délibérément tenté d'entraver la procédure de contrôle. Ainsi, SAF LOGISITIC n'a traduit que partiellement le formulaire qui était rédigé en langue chinoise. Ainsi les champs relatifs à l'appartenance ethnique ou l'affiliation politique étaient manquants. A noter que le manque de coopération constitue un facteur aggravant lors de la détermination du montant de la sanction par l'autorité de contrôle.

2) LE RESPONSABLE DE TRAITEMENT ET LE SOUS-TRAITANT SONT RESPONSABLES EN CAS DE NON-CONCLUSION D'UN ACCORD DE PROTECTION DES DONNEES

Le 29 septembre 2023, l'Autorité de Protection des Données belge (APD) a rendu une décision apportant des éclairages intéressants sur d'une part les obligations à la charge du responsable de traitement et du sous-traitant et d'autre part sur la correction tardive des manquements au RGPD. A cet égard, l'ADP a indiqué que :

- **Le responsable du traitement et le sous-traitant ont tous deux violé les dispositions de l'article 28 du RGPD en ne concluant pas d'accord de protection des données** (DPA) dès le début du traitement de données. L'obligation de conclure un contrat ou d'être lié par un acte juridique contraignant pèse à la fois sur le responsable du traitement et sur le sous-traitant et non sur le seul responsable du traitement.
- **La clause de rétroactivité prévue au sein des DPA n'est pas de nature à pallier l'absence de contrat au moment des faits** : seule la date de signature du DPA doit être prise en compte pour déterminer la conformité du traitement concerné. L'ADP rappelle que si une telle rétroactivité devait être admise, elle permettrait de facto de contourner l'application dans le temps de l'obligation de l'article 28.3. du RGPD. Or, le RGPD a lui-même prévu un délai de 2 ans séparant son entrée en vigueur de son entrée en application pour une mise en conformité progressive par toutes les entités concernées en vue de garantir la protection des droits et des personnes concernées.

3) UNE NOUVELLE PLAINTE VISE LA START-UP D'OPENAI A L'ORIGINE DE L'INTELLIGENCE ARTIFICIELLE GENERATIVE CHATGPT

L'Office polonais pour la protection des données a ouvert une enquête à la suite du dépôt de plainte du chercheur polonais, Lukasz Olejnik contre la start-up Open AI en septembre 2023. Cette plainte met en exergue les multiples manquements du chatbot au respect du Règlement général sur la protection des données (RGPD).

Les manquements au RGPD soulevés par la plainte

La plainte recense de nombreuses infractions au RGPD, notamment une violation des articles suivants :

- L'article 5 relatif à l'obligation d'exactitude des données et le traitement loyal de celles-ci (il existe une obligation de limitation des finalités) ;
- L'article 6 relatif à la base légale du traitement ;
- Les articles 12 et 14 relatifs à l'information des personnes concernées ;
- L'article 15 sur le droit d'accès pour la personne concernée aux informations sur le traitement de ses données ;
- L'article 16 sur le droit pour les personnes concernées de rectifier les données à caractère personnel qui sont inexactes.

Les intérêts légitimes poursuivis par OpenAI semblent difficilement contrebalancer les atteintes portées à la vie privée des utilisateurs.

Des plaintes répétées à l'encontre d'OpenAI

Ce n'est pas la première fois que, depuis sa mise en ligne, le logiciel ChatGPT est visé par de telles accusations. A l'échelle mondiale, huit plaintes ont été déposées cette année en raison de manquements à la protection des données personnelles. Sont notamment relevés :

- L'absence de consentement des personnes dans le traitement de leurs données
- Le traitement inexacte des données
- L'absence de filtre permettant de vérifier l'âge des individus
- Le non-respect du droit à l'opposition.

La technique du « *scraping* », dont cette intelligence artificielle fait usage (technique qui permet une extraction automatique de nombreuses informations issues d'un ou plusieurs sites web) a été signalée par la CNIL dès 2020 dans une série de recommandations visant à encadrer ladite pratique dans le cadre de la prospection commerciale. Ces contrôles avaient mené la CNIL à soulever divers manquements à la législation sur la protection des données, tels que :

- L'absence d'information des personnes visées par le démarchage ;
- L'absence de consentement des personnes avant leur démarchage ;
- L'absence du respect de leur droit d'opposition.

Vers un meilleur encadrement de l'intelligence artificielle ?

En avril 2021, la Commission européenne a fait une proposition de règlement précisant de nouvelles mesures afin de veiller à ce que les systèmes d'intelligence artificielle utilisés dans l'Union Européenne soient sûrs, transparents, éthiques et sous contrôle humain. Ce règlement prévoit un classement de systèmes à haut risque, risque limité et risque minimal, en fonction de leurs caractéristiques et finalités.

En attendant l'entrée en vigueur de ce règlement, la CNIL veille à apporter des réponses concrètes aux problématiques portées par l'intelligence artificielle. A ce titre, elle a déployé en mai 2023 un plan d'action destiné à devenir un cadre de régulation dont l'objectif est de permettre le déploiement opérationnel de systèmes d'intelligence artificielle respectueux des données personnelles.

---

[1]En mars dernier, la CNIL italienne est allée jusqu'à suspendre temporairement ChatGPT sur son territoire en raison d'une présomption de violation des règles de l'Union européenne en matière de protection des données.

OpenAI omis de mettre en place un système de vérification de l'âge des utilisateurs. Dans la continuité de cet évènement, un recours collectif américain a dénoncé le 28 juillet dernier l'accessibilité des services aux mineurs de moins de 13 ans ainsi que l'utilisation de méthodes de « *scraping* » auprès de plateformes telles qu'Instagram, Snapchat ou même Microsoft Teams.

[2]Proposition de règlement établissant des règles harmonisées concernant l'intelligence artificielle

4) TRANSFERT DE DONNEES VERS LES ETATS-UNIS

La Commission européenne a adopté le 10 juillet 2023 une nouvelle décision d'adéquation permettant les transferts de données transatlantiques, dénommée « Data Privacy Framework » (**DPF**).

Depuis le 10 juillet, il est ainsi possible pour les entreprises soumises au RGPD de transférer des données personnelles aux sociétés américaines certifiées « DPF » sans recourir aux clauses contractuelles types de la Commission européenne et aux mesures supplémentaires. Cela a été rappelé par le CEPD le 18 juillet 2023[1].

A noter que le Royaume-Uni a également conclu un accord avec les Etats-Unis relatif au transfert de données qui entrera en vigueur le 12 octobre prochain.

Pour rappel, la Cour de justice de l'Union européenne (**CJUE**) avait invalidé dans un arrêt du 16 juillet 2020 le « *Privacy Shield* », la précédente décision d'adéquation qui permettait le transfert des données personnelles vers les Etats-Unis.

1) Le contenu du « Data Privacy Framework »

La décision du 10 juillet 2023 formalise nombre de garanties contraignantes pour tenter de remédier aux faiblesses du « *Privacy Shiel*d » invalidé deux ans auparavant.

a) Les nouvelles obligations

Afin de se prévaloir de ce nouveau cadre et être destinataire de données personnelles de résidents européens, les entreprises américaines devront notamment :

- Déclarer adhérer aux principes de protection des données personnelles du DPF (minimisation des données, durées de conservation, sécurité…).
- Indiquer un certain nombre d'informations obligatoires : le nom de l'organisation concernée, la description des finalités pour lesquelles le transfert de données personnelles est nécessaire, les données personnelles couvertes par la certification ainsi que la méthode de vérification choisie.
- Formaliser une politique de confidentialité conforme aux principes du DPF et préciser le type de recours indépendant pertinent offert aux détenteurs premiers des données, ainsi que l'organe statutaire compétent pour assurer le respect de ces principes.

Le Ministère du Commerce américain *(US Department of Commerce)* a ouvert le lundi 17 juillet le site web du programme « *Data Privacy Framework* », qui offre aux entreprises un guichet unique où elles peuvent adhérer au DPF et répertorie la liste des entreprises qui y ont adhéré.

Les entreprises américaines adhérentes doivent conduire chaque année des auto-évaluations afin de démontrer leurs respects aux exigences du DPF. En cas de violation de ces principes, le Ministère du Commerce américain peut infliger des sanctions.

Il convient de noter que les entreprises déjà affiliées au *Privacy Shield* sont automatiquement affiliées au DPF sous réserve de mettre à jour leur politique de confidentialité avant le 10 octobre 2023.

b) La création d'une Cour de révision de la protection des données

Le DPF se montre innovant puisqu'il instaure une Cour de révision de la protection des données (**Data Protection Review Court, DPRC**) permettant à la fois un accès facilité, impartial et indépendant à des recours pour les résidents de l'Union européenne mais aussi une prise en charge effective des manquements aux règles issues du cadre UE-Etats-Unis. Cette Cour est en effet dotée de pouvoir d'enquête et peut ordonner des mesures correctives contraignantes, telle que, par exemple, la suppression des données importées illégalement.

c) Un nouveau mécanisme de recours pour les ressortissants de l'Union européenne

Le mécanisme de recours prévu s'effectuera à deux niveaux :

- Dans un premier temps, la réclamation sera portée auprès de l'autorité nationale compétente (par exemple, la CNIL en France). Cette autorité sera le point de contact du plaignant et lui transmettra toutes les informations relatives à la procédure. La réclamation est communiquée aux Etats-Unis via le Comité européen de la protection des données (**CEPD**) où elle est examinée par **le délégué à la protection des libertés** qui statue sur l'existence ou non d'une violation.

- Le plaignant pourra faire appel de la décision du délégué à la protection des libertés civiles devant la DPRC. La DPRC sélectionnera dans chaque cas un « *special advocat* » ayant l'expérience requise pour assister le plaignant.

D'autres voies de recours comme l'arbitrage sont également disponibles.

2) Les évolutions à venir : de nouvelles batailles judiciaires ?

Ce nouveau cadre juridique sera soumis à des examens périodiques, le premier étant prévu l'année suivant l'entrée en vigueur de la décision d'adéquation. Ces contrôles seront réalisés à la fois par la Commission européenne, les autorités américaines compétentes (U.S. Department of Commerce, Federal Trade Commission et le U.S. Department of Transportation) mais aussi par divers représentants des autorités européennes de protection des données.

Malgré la mise en place de ces nouveaux garde-fous, la riposte judiciaire a déjà eu lieu.

Le 6 septembre dernier, le député français Philippe Latombe (MoDem) a déposé deux plaintes auprès de la CJUE en vue d'obtenir l'annulation du DPF. Max Schrems, président de l'association autrichienne de défense de la vie privée « Noyb », à l'origine des recours contre les anciens accords (Safe Harbor et Privacy Shield), devrait très probablement lui emboîter le pas.

5) QUESTIONS AUTOUR DU CHAMP D'APPLICATION MATERIEL DU RGPD

Une position clivante d'un avocat général concernant le champ d'application matériel du RGPD, pourrait, si elle est suivie par la CJUE, limiter nettement l'application du RGPD à de nombreux secteurs d'activité (affaire C-115/22).

En l'espèce, les nom et prénom d'une sportive autrichienne testée positive au contrôle antidopage avait été publié sur le site Internet accessible au public de l'Agence indépendante de lutte contre le dopage autrichienne (NADA).

La sportive a saisi la Commission indépendante d'arbitrage autrichienne (l'USK) d'une demande de réexamen de cette décision. Cet organe s'interroge notamment sur la compatibilité avec le RGPD de la publication sur Internet des données à caractère personnel d'un sportif professionnel dopé. Un renvoi préjudiciel auprès de la CJUE est alors effectué.

L'avocat général considère que le RGPD n'est pas applicable en l'espèce dans la mesure où les règles antidopage réglementent essentiellement les fonctions sociales et éducatives du sport plutôt que ses aspects économiques. Or, il n'existe actuellement aucune règle de droit de l'Union relative aux politiques de lutte contre le dopage des États membres. À défaut de lien entre les politiques de lutte contre le dopage et le droit de l'Union, le RGPD ne saurait régir de telles activités de traitement.

Cette analyse de fonde sur l'article 2.2.a) du RGPD qui prévoit :

« Le présent règlement ne s'applique pas au traitement de données à caractère personnel effectué :

a) dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union; »

Les contours du champ d'intervention de l'Union sont variables et imprécis, entraînant en conséquence une incertitude quant à l'application du RGPD à certains secteurs.

À titre subsidiaire et si le RGPD devait s'appliquer, l'avocate générale considère en tout état de cause que la décision du législateur autrichien d'imposer la divulgation au public des données à caractère personnel des sportifs professionnels violant les règles antidopage applicables n'est pas, aux termes du règlement, subordonnée à un examen de proportionnalité.

Les conclusions de l'avocat général ne lient toutefois pas la CJUE. La décision de la juridiction européenne est en conséquence attendue avec attention, en ce qu'elle permettra de préciser les contours de l'application du RGPD.

Emilie de VAUCRESSON
Avocate associée
edevaucresson@joffeassocies.com

Amanda DUBARRY
Avocate
adubarry@joffeassocies.com

Camille LEFLOUR
Avocate
cleflour@joffeassocies.com