ACTUALITÉS AVRIL 2022

1. Données de trafic

Au terme d'un arrêt rendu par la Grande chambre de la Cour de justice de l'Union européenne, au sujet de l'affaire Graham Dwyer (du nom du meurtrier condamné à la suite de l'exploitation des métadonnées contenues dans son téléphone), il a été jugé, que l'article 15§1 de la directive 2002/58/CE du 12 juillet 2002 sur la vie privée et les communications électroniques (modifiée par la directive 20009/136/CE), lu, à la lumière des articles 7,8 et 11 de la Charte des droits fondamentaux de l'Union européenne s'oppose à ce que des mesures législatives nationales prévoient, à titre préventif, aux fins de la lutte contre la criminalité grave et la prévention des menaces contre la sécurité publique, une conservation généralisée et indifférenciée des données de trafic et de localisation*.
Le principe est donc celui d'une interdiction de stockage de telles données.
Pour rappel, il s'agit d'une confirmation de la jurisprudence de la Cour de justice en matière de données de trafic.
La Cour de justice a, en revanche, précisé que ces mêmes dispositions ne s'opposent pas, sous réserve de règles claires et précises, à :

- une conservation ciblée des données de trafic et de localisation, délimitée sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable ;
- une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire ;
- une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs au moyen de communications électroniques ;
- le recours à une injonction faite aux fournisseurs de services de communications électroniques, au moyen d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont disposent ces fournisseurs de services.

Ces mesures doivent néanmoins assurer que la conservation de telles données soit subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus.

CJUE, gde ch. 5 avr. 2002, aff. C-140/20

**données permettant d'identifier et de localiser les utilisateurs ou les destinataires d'un appel, la date, l'horaire, la durée de chaque communication passée par un utilisateur de téléphone mobile.*

2. Localisation des données et contrats conclus avec le secteur public britannique

La question relative à la localisation des données semblerait intégrer, de plus en plus, la sphère des contrats conclus avec le secteur public britannique et les agences gouvernemenatales.
Selon l'association teckUK (association britannique regroupant notamment des entreprises de la technologie), la garantie d'une localisation des données au Royaume-Uni serait de plus en plus exigée.

Un porte-parole du gouvernement a toutefois démenti l'existence d'une telle exigence, arguant que chaque département doit prendre en compte les principes de sécurité du Cloud élaborés par le National Cyber Security Center lorsqu'ils envisagent la conclusion d'un contrat de nature commerciale.

3. Google : rajout d'un bouton au sein du bandeau cookies pour l'Europe

Dans le prolongement de l'amende d'un montant de 150 millions d'euros prononcée par l'autorité de protection des données française (CNIL), Google a annoncé, le 21 avril dernier, la mise en place d'un bouton permettant aux internautes d'accepter, de personnaliser le suivi ou de refuser tous les cookies (ce qui devrait empêcher le dépôt de cookies de tracking publicitaire et l'affichage d'un contenu personnalisé).
Rappelons que jusqu'à récemment, ces derniers étaient contraints soit d'accepter les cookies soit de les personnaliser.
Or, l'amende prononcée à l'encontre du géant américain a été assortie d'une astreinte de 100 000 euros par jour de non-conformité passé un délai de 3 mois à compter du prononcé de la sanction.
Aucune date concernant le déploiement de cette mise à jour n'a pour le moment été communiquée.

L'Autorité allemande de protection des données a accueilli favorablement le projet de bouton *« refuser tous les cookies ».*

4. Juridictions du pays voisin

- Le Tribunal judiciaire de Paris a, par ordonnance du 5 avril 2022, ordonné à un opérateur de réseau mobile, de communiquer l'ensemble des données qu'il détient pour permettre d'identifier le titulaire d'un numéro de téléphone qu'il gère. Le tribunal a en effet estimé que la demande de communication était proportionnée aux intérêts en présence et nécessaire au droit de la preuve.

- Le Tribunal judiciaire de Strasbourg a, par ailleurs, eu l'occasion de rappeler, au sujet de la fourniture d'un progiciel de gestion intégrée (ERP) et de la vente d'un matériel informatique financée par un contrat de leasing, que le client est tenu de vérifier l'adéquation dudit logiciel à ses besoins.
  Le client a donc en l'espèce été condamné à honorer les sommes dues au titre des loyers échus impayés et de l'indemnité de résiliation ainsi qu'à restituer le matériel objet du contrat.
  Les contrats de fourniture du progiciel, de fourniture du matériel informatique et de location financière ont par ailleurs été reconnus comme étant interdépendants les uns des autres, de telle sorte que si le client avait pu justifier de manquements imputables à son fournisseur s'agissant du progiciel (manquement du fournisseur à son obligation de conseil et manquement à son obligation d'information) la résiliation du contrat de fourniture aurait pu entrainer la caducité des deux autres.
  Aucun manquement n'a en revanche été rapporté par le client, ce dernier aurait dû vérifier l'adéquation des progiciels à ses besoins. Le tribunal a d'ailleurs retenu que le client utilisait ce type de logiciel depuis une dizaine d'années et qu'il n'avait que tardivement fait connaître ses griefs au fournisseur.

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

- **Belgique**

  Contrôles de température dans les aéroports :

  L'autorité de protection des données belge a infligé une amende de 200.000 euros à Brussels Airport Zaventem et de 100.000 euros à l'aéroport Brussels South Charleroi en raison de contrôles de température des passagers effectués dans le cadre de la lutte contre la COVID-19. Pour l'APD, ces aéroports ne disposaient pas d'une base légale valable pour traiter des données de santé des voyageurs. Or, ces aéroports filtraient, à l'aide de caméras thermiques, les passagers présentant plus de 38° de température. Une fois filtrées, les personnes devaient remplir un questionnaire portant sur de possibles symptômes liés au virus.

  Pour rappel, les données de santé, sont des données sensibles qui ne peuvent être traitées que dans un nombre limité de cas (article 12 de la Loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives et article 9 du Règlement Général à la Protection des Données).

- **France**

  Prospection commerciale : Des mises en demeure ont récemment été adressées à plusieurs sociétés. Ces dernières font suite à la transmission à certains de leurs partenaires des données personnelles de prospects, sans recueil de consentement. Les organismes sanctionnés disposent désormais de 3 mois pour se conformer à la règlementation.

  Fuite de données médicales : Une amende d'un montant de 1,5 million d'euros a été infligée à la société Dedalus qui édite des logiciels notamment destinés aux laboratoires d'analyses médicales.

  Le prononcé de cette amende fait suite à la fuite de données médicales concernant près de 500 000 français, laquelle avait été médiatisée en février 2021. En effet, outre des informations relatives aux noms, prénoms, adresses et téléphones de patients, s'étaient également retrouvées en libre accès des données hautement plus sensibles comme le groupe sanguin, le numéro de sécurité sociale ou les pathologies des patients (cancers, VIH, maladies génétiques, grossesses, traitements médicaux suivis ou encore données génétiques).

  Des opérations de contrôle avaient été menées, par l'autorité de protection des données française (CNIL), auprès de l'éditeur de logiciels, la source de la fuite ayant rapidement été identifiée comme provenant du logiciel de la société Dedalus.

  A l'issue de ces opérations de contrôle, la CNIL avait relevé de nombreux manquements aux obligations prévues par le Règlement européen à la protection des données parmi lesquels :

  - un manquement à l'obligation pour le sous-traitant de respecter les instructions du responsable de traitement, Dedalus Biologie ayant traité des données au-delà des instructions données par les laboratoires responsables de traitement ;
  - un manquement à l'obligation d'assurer la sécurité des données en mettant en place des mesures techniques et organisationnelles appropriées (absence de procédure spécifique pour la migration de données, absence de chiffrement des données stockées sur le serveur problématique, absence effacement automatique des données après leur migration, absence d'authentification requise pour accéder à la zone publique du serveur, etc.) ;
  - un manquement à l'obligation d'encadrer par un acte juridique formalisé les traitements effectués pour le compte du responsable de traitement.

  Pour d'information la délibération de la CNIL est disponible ICI.

- **Hongrie**

  Usage illicite de l'intelligence artificielle

  Une amende d'un montant de 670.000 euros a été prononcée par l'autorité hongroise de protection des données à l'égard d'un établissement bancaire.

  Il lui était reproché d'analyser de manière automatique l'ensemble des appels passés au service clientèle.

  Les résultats de ces analyses lui permettaient de déterminer (en fonction de l'analyse de l'état émotionnel de l'appelant par le biais d'un logiciel de traitement du signal vocal basé sur l'IA et d'une liste de mots-clés) quels clients devaient être rappelés.

  Le logiciel permettait, par la suite, d'établir un classement des appels servant de recommandation pour déterminer quel appelant devait être rappelé en priorité.

  D'après la banque, ce traitement se justifiait par un intérêt légitime de l'établissement de contrôle de qualité sur la base de paramètres variables, de prévention des plaintes et de la migration des clients.

  L'Autorité de protection des données a cependant relevé que la notice de confidentialité de la banque (Privacy Notice) ne faisait référence à ces activités de traitement qu'en des termes généraux, aucune information matérielle n'étant disponible s'agissant de l'analyse vocale en elle-même. En outre, cette dernière ne mentionnait que le contrôle de la qualité et la prévention des plaintes comme finalités du traitement. Les personnes concernées ne disposaient dès lors pas de la possibilité de refuser l'analyse vocale effectuée.

  Or, l'Autorité de protection a rappelé que la seule base juridique pour ce type de traitement (traitement d'analyse vocale basée sur les émotions) est le consentement libre et éclairé des personnes concernées. En outre, elle a retenu, qu'en dépit d'une analyse d'impact ayant mis en avant les risques importants liés à ce traitement, la banque n'a pas été en mesure de présenter des solutions permettant de remédier à ces risques.

- **Danemark**

  La plus importante banque danoise « *Dankse Bank* » fait actuellement face à un risque d'amende de 10 millions de couronnes danoises pour diverses violations du RGPD en lien avec le stockage de données de ses clients.

  En effet, il est apparu que la banque stockait ces données pour une durée excessive et ne procédait pas à leur suppression comme l'exige le règlement européen.

  Pour rappel, en vertu du RGPD, les données personnelles doivent, hormis quelques exceptions prévues par le texte parmi lesquelles le respect d'une obligation légale, être supprimées, par les fournisseurs de services, à la fin des services ou à l'expiration d'un accord juridique.

Commission de Contrôle des Informations Nominatives
Ce document est à vocation purement informative et ne peut être considéré comme reflétant une position officielle de la CCIN