CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Communication présentée en séance plénière le 11 janvier 2024

Quel régime juridique pour la protection des données après le Brexit ?

Présentation du projet de nouvelle loi britannique sur la protection des données

Rapporteur : M. Bertrand du Marais

Avec le concours de : [redacted]

Table des matières

Résumé / synthèse de la position de la CNIL

La loi sur la protection des données et l'information numérique du Royaume-Uni est en cours de discussion. Mise en chantier depuis plusieurs mois, compte tenu notamment des changements successifs de Premier ministre, elle pourrait être adoptée au cours de l'année 2024. La loi vise notamment à simplifier les obligations légales pour les entreprises. Dans cet esprit, la manière dont évoluera le texte au fil de la discussion parlementaire sera suivie de près par la Commission européenne et l'ensemble des Autorités de protection des données européennes œuvrant ensemble dans le Comité européen pour la protection des données.

I- Rappel du contexte

A- Rappel sur le cadre juridique en matière de protection des données au Royaume-Uni) [1]

À ce jour, le Royaume-Uni fonctionne avec plusieurs régimes réglementaires.

En 2018, avec l'entrée en application du RGPD au Royaume-Uni, une nouvelle loi a été introduite en abrogeant la loi de 1998 transposant la directive 95/46/CE et en introduisant des dérogations et des spécifications là où le texte du RGPD le permettait.

Ces dispositions sont regroupées au sein de la 2e partie du Data Protection Act de 2018, les conventions et actes internationaux n'étant pas d'application directe en raison de l'appartenance du Royaume-Uni au principe de dualisme en droit international.

Les dispositions de la directive « Police- Justice » ont été transposées en droit britannique dans la 3e partie de ce texte.

Le cadre juridique applicable aux services de renseignement est déterminé dans la 4e partie de la loi.

A la suite du Brexit, en vertu de la section 3 du Traité de sortie de l'Union européenne (*European Union Withdrawal Act 2018 (EUWA 2018)*), le RGPD a été incorporé dans le droit britannique.

Le cadre juridique a été modifié par le *Data Protection Act, Privacy and Electronic Communication (Amendments etc) (EU Exit) Regulations 2019*, qui a ainsi créé le « UK – GDPR ». Il est entré en vigueur à la fin de la période de transition, le 1er janvier 2021.

Le cadre juridique en matière de protection des données du Royaume-Uni comprend donc plusieurs régimes réglementaires :

- le régime général est régi par le « UK- GDPR » et la 2e partie du DPA 2018, ce régime est quasi identique du RGPD ;
- les traitements par les autorités compétentes à des fins répressives (police-justice) sont régis par la 3e partie du DPA 2018 ;
- les traitements par les services de renseignement britanniques sont régis par la 4e partie du DPA 2018 ;
- les règles relatives aux communications électroniques introduites par la directive 2002/58/EC (dite « ePrivacy ») ont été transposées en droit britannique au sein des *Privacy and Electronic Communications (EC Directive) Regulations 2003*.

[1] Notes explicatives qui accompagnent le projet de loi [Explanatory Notes related to the Data Protection and Digital Information Bill as brought from the House of Commons on 6 December 2023 (HL Bill 30], disponibles ici, paragraphes 82 – 87

La Commission européenne (CE) a adopté deux décisions d'adéquation pour le Royaume-Uni, l'une au titre du RGPD[2] et l'autre au titre de la directive « Police - Justice »[3].

B- Le projet de loi (*Data Protection and Digital Information Bill*) apporte des modifications à tous ces textes.

Après ces prédécesseurs, le gouvernement britannique de M. Sunak a introduit, le 8 novembre 2023, un **projet de loi sur la protection des données et information numérique** (*Data Protection and Digital Information Bill*[4], *DPDI*). Le nouveau projet de loi vise à mettre à jour et à simplifier le cadre de protection des données du Royaume-Uni en modifiant certaines dispositions[5]. L'objectif du projet de loi est d'apporter de la flexibilité et de réduire les charges organisationnelles tout en maintenant des normes élevées en matière de protection des données.

C- Examen du processus législatif jusqu'à la promulgation de la loi [6]

Le 29 novembre 2023, le projet de loi a été lu pour la troisième fois par la Chambre des communes. La Chambre des Lords a lu le texte une deuxième fois le 19 décembre 2023[7]. Le projet de loi continuera à faire l'objet d'un va-et-vient entre chaque chambre jusqu'à ce que les deux chambres parviennent à un accord. Ce n'est qu'ensuite que le texte reçoit la « sanction royale » avant de devenir une loi.

La loi pourrait être définitivement adoptée dans le courant de l'année 2024. La législature sortante doit être dissoute au plus tard le 17 décembre 2024.

II- Les critiques du gouvernement sur le cadre juridique existant et les objectifs de la nouvelle loi

A- Les critiques gouvernementales portent sur les conséquences économiques du respect de la protection des données

Le gouvernement britannique est assez critique vis-à-vis du cadre juridique existant qu'il estime lourd et difficilement applicable. Selon son analyse, certains éléments de

---

[2] Commission européenne, Décision d'exécution de la Commission constatant le niveau de protection adéquat des données personnelles assuré par le Royaume-Uni (au titre du RGPD), disponible ici

[3] Commission européenne, Décision d'exécution de la Commission constatant le niveau de protection adéquat des données personnelles assuré par le Royaume-Uni (au titre de la directive 2016/680), disponible ici

[4] Le projet, tel qu'il a été introduit, disponible ici. Sa dernière version telle qu'introduite par la Chambre des communes à la Chambre des lords le 6 décembre 2023, disponible ici

[5] Il est difficile de naviguer le projet de loi et comprendre les modifications apportées à chaque article. Notre analyse est basée pour la plus grande partie sur la dernière version des notes explicatives qui accompagnent le projet de loi [*Explanatory Notes related to the Data Protection and Digital Information Bill as brought from the House of Commons on 6 December 2023 (HL Bill 30*], disponibles ici

[6] Le processus législatif britannique est expliqué par le site du Parlement ici

[7] Le processus législatif de ce projet de loi est décrit ici

la législation créent « *des obstacles, de l'incertitude et des charges inutiles pour les entreprises et les consommateurs* ».

Parmi les plus importantes critiques, les Notes explicatives qui accompagnent le projet de loi mentionnent que [8] :

- Le cadre juridique applicable créerait une incertitude quant aux différentes bases juridiques sur lesquelles les entreprises privées se fondent pour traiter des données à caractère personnel à la demande d'organismes publics. Cela peut créer une charge inutile pour les organisations privées et ralentir la fourniture des services publics.
- La législation actuelle prescrirait une série d'activités et de contrôles que les organisations doivent réaliser pour être considérées comme conformes. Cette approche, selon le gouvernement, peut tendre vers un régime de conformité de type "case à cocher", plutôt que vers un régime qui encourage une approche proactive et systémique.
- La législation actuelle ne fournirait pas à l'autorité de protection des données britannique (l'ICO) un cadre suffisamment clair d'objectifs et de devoirs en rapport avec ses responsabilités en matière de protection des données. Ceci l'empêcherait de hiérarchiser ses activités et ses ressources, d'évaluer ses performances et d'être tenue pour responsable par les parties prenantes. Au contraire, l'ICO serait tenu de remplir une longue liste de tâches, comme le prévoit l'article 57 du UK GDPR, mais sans cadre stratégique pour guider son travail.

En réponse, selon le Gouvernement, le projet de loi :

- clarifie la formulation du cadre juridique afin d'aider les chercheurs dans leur utilisation des données personnelles. Il permettrait la réutilisation des données personnelles à des fins d'études à plus long terme.
- rationalise les exigences que la législation actuelle impose aux organisations pour démontrer qu'elles se conforment à la législation. Il modifie également l'exemption que les organisations peuvent invoquer pour facturer une redevance raisonnable ou refuser de répondre à une demande d'exercice de ses droits d'une personne concernée lorsque la demande est jugée "vexatoire ou excessive" (*'vexatious or excessive'*).
- modifie le règlement de 2003 sur la protection de la vie privée et les communications électroniques (Privacy and Electronic Communications Regulations 2003), en ce qui concerne la confidentialité des équipements terminaux (par exemple, les règles relatives aux cookies), les communications (par exemple, les appels intempestifs) et la sécurité des communications (par exemple, le trafic réseau et les données de localisation).
- clarifie les règles relatives aux transferts internationaux et aux flux transfrontaliers de données à caractère personnel. Le régime réformé vise à continuer à garantir des normes de protection élevées lorsque les données des personnes sont transférées à l'étranger. Les tests de protection des données se concentreront sur les résultats obtenus en matière de protection des données pour les personnes concernées, quelle que soit la forme du transfert.

[8] Notes explicatives, paragraphes 13-20

B- Des modifications substantielles sont apportées s'agissant des activités régaliennes[9]

La nouvelle loi vise aussi à harmoniser certaines dispositions « Police-Justice » qui existent dans le Data Protection Act et le UK GDPR[10]. Parmi les modifications, le projet vise à « simplifier » le régime applicable aux services de renseignement britannique. Selon le gouvernement, « *la situation actuelle, dans laquelle les services répressifs et les services de renseignement sont régis par des régimes de protection des données différents, pose des problèmes au travail opérationnel commun de ces services* ».

En outre, les modifications introduites par le projet de loi devraient permettre une mise en œuvre rapide des nouveaux accords internationaux en matière de répression et d'échange d'informations.

La législation vise aussi à alléger les conditions qui permettent au ministère du Travail et des pensions (DWP) de demander à des tiers des informations sur des bénéficiaires des prestations sociales, soupçonnées de fraude.

Le projet introduit des obligations pour les réseaux sociaux afin d'aider les services compétents à investiguer les morts de mineurs.

Enfin, le gouvernement estime que les dispositions actuelles en matière de contrôle de l'utilisation par la police des données biométriques et des caméras de surveillance, destinées à aider à identifier et à éliminer les suspects sont complexes et déroutantes pour la police (en tant que RT) et pour le grand public. Le projet de loi simplifiera le cadre de contrôle de l'utilisation par la police des données biométriques et de l'utilisation par la police et les autorités locales des caméras de surveillance.

C- Autres dispositions

Le projet de loi introduit d'autres dispositions diverses concernant :

- un nouveau cadre réglementaire pour la fourniture de services de vérification numérique au Royaume-Uni et l'autorisation pour les autorités publiques de divulguer des informations personnelles à des fournisseurs de services de vérification numérique de confiance à des fins de vérification de l'identité et de l'éligibilité ;
- la possibilité pour les employeurs et les propriétaires qui louent leur bien de faire appel à des fournisseurs de services de vérification numérique pour effectuer les contrôles d'identité des salariés et locataires respectivement ;
- l'amélioration de la qualité (standardisation) des données traitées par les services sociaux pour faciliter leur partage ;
- des dispositions permettant l'exercice effectif du droit à la portabilité des données (*Smart Data Schemes*), notamment dans le secteur bancaire

[9] Notes explicatives, paragraphes 91 - 127
[10] Notes explicatives, paragraphes 21-25

III- Les plus importantes modifications proposées en détail

Le projet de loi n'est pas facile à lire. En effet, plutôt que de remplacer la législation existante, le législateur a choisi de modifier le « UK GDPR » et la Data Protection Act 2018, ce qui signifie que les lecteurs doivent faire des références croisées entre trois textes (plus les notes explicatives et l'analyse d'impact de la loi).

A- Modification de la définition d'une personne « identifiable » (Section 1)

Le législateur souhaite ajouter des précisions quant au cas d'identification indirecte d'une personne. Une personne est considérée comme identifiable si le responsable de traitement ou le sous-traitant peut l'identifier à travers d'autres informations qu'ils ont à leur disposition en utilisant des moyens raisonnables ou si une tierce personne destinataire des données peut identifier cette personne en utilisant des moyens raisonnables.

Une personne est identifiable « en utilisant des moyens raisonnables » si elle est identifiable en utilisant des moyens que le responsable de traitement ou le sous-traitant est « raisonnablement susceptible » d'utiliser.

La question de savoir si un responsable du traitement ou un sous-traitant est « raisonnablement susceptible d'utiliser un moyen d'identification d'une personne » doit être déterminée en tenant compte, entre autres des éléments suivants : a) le temps, les efforts et les coûts liés à l'identification de la personne par ce moyen, et b) la technologie et les autres ressources dont dispose le responsable de traitement ou le sous-traitant.

B-Finalités ultérieures compatibles avec les traitements initiaux (Section 6 & Annexe 2)

Le projet de loi ajoute des indices pour aider les responsables de traitement à déterminer si les finalités ultérieures sont compatibles avec les finalités initiales des traitements. La loi énumère aussi en annexe des finalités ultérieures qui sont compatibles avec les finalités d'origine poursuivies par le responsable de traitement.

C-Simplification des formalités pour l'utilisation de l'intérêt légitime comme base légale et élargissement des intérêts légitimes reconnus (Section 5 & Annexe 1)

Une liste exhaustive d'intérêts légitimes qui « passent » automatiquement le test de mise en balance de ces intérêts avec les droits et libertés des personnes concernées figure en annexe.

La liste contient des traitements mis en place sous certaines conditions pour (i) la sécurité nationale, la sécurité publique et la défense (ii) les cas d'urgence (iii) la lutte contre la criminalité (iv) la sauvegarde des personnes vulnérables, et (v) la participation à la vie démocratique.

Une procédure est également prévue pour ajouter à l'avenir d'autres finalités à cette liste y compris par actes administratifs émis par le Secrétaire d'État (le ministre compétent).

D- Clarification du terme « recherche » (Section 2)

S'agissant de la recherche, trois nouvelles définitions ont été ajoutées ayant pour objectif d'apporter une plus grande clarté au cadre juridique applicable.

Le traitement à des fins de "recherche scientifique" est défini comme "le traitement à des fins de toute recherche pouvant raisonnablement être qualifiée de scientifique, qu'elle soit financée par des fonds publics ou privés, y compris le traitement à des fins de développement ou de démonstration technologique, de recherche fondamentale ou de recherche appliquée". Cela inclut uniquement les études de santé publique lorsque l'étude est menée dans l'intérêt public.

Le traitement à des fins de « recherche historique » est défini comme « comprenant le traitement à des fins de recherche généalogique ».

Le traitement à des « fins statistiques » est défini comme « le traitement à des fins d'enquêtes statistiques ou de production de résultats statistiques lorsque - (a) les informations qui résultent du traitement sont des données agrégées qui ne sont pas des données à caractère personnel, et (b) ni ces informations, ni les données à caractère personnel traitées, ne sont utilisées à l'appui de mesures ou de décisions concernant une personne physique en particulier ».

E- Interprétation large du consentement comme base légale pour effectuer de la recherche scientifique (Section 3)

Le consentement de la personne à des finalités de recherche scientifique sera considéré comme valide lorsque (i) au moment de la collecte, il était impossible de déterminer de manière exhaustive les finalités de la recherche, (ii) la recherche respecte les standards éthiques reconnus dans le domaine de cette recherche, (iii) la personne concernée peut consentir uniquement au traitement pour une partie de la recherche.

[redacted] Il s'agit d'une reprise des éléments du considérant 33 du RGPD.

F- Possibilité pour les responsables de traitement de refuser les demandes vexatoires ou excessives (Section 9)

Le seuil pour refuser les demandes d'exercice des droits par les personnes concernées est passé de "manifestement infondé" à "vexatoire ou excessif". Chaque demande doit être évaluée au cas par cas en tenant compte de facteurs tels que la relation entre le responsable du traitement et la personne concernée, les ressources dont dispose le responsable du traitement et le délai entre les demandes.

Parmi les exemples de demandes qui atteindront ce seuil, on peut citer celles qui sont destinées à causer un désagrément, qui ne sont pas faites de bonne foi ou qui constituent un abus de procédure.

Cette modification devrait donc permettre aux responsables du traitement de refuser plus facilement certaines demandes.

G- Limitation du droit de ne pas être soumis à une décision automatisée (Section 14)

Les dispositions relatives à la prise de décision automatisée ont été remplacées dans leur intégralité.

La définition de "uniquement automatisée" a été clarifiée pour signifier une décision dans laquelle il n'y a "aucune implication humaine significative".

L'interdiction générale des décisions automatisées ne s'applique plus que lorsque de telles décisions sont fondées en tout ou en partie sur des catégories particulières de données à caractère personnel. Dans ces circonstances, une décision automatisée ne peut être prise que si (i) la personne concernée a donné son consentement ; ou (ii) la décision est nécessaire à l'exécution d'un contrat ou exigée par la loi et qu'une condition d'intérêt public important s'applique.

Les personnes concernées auront le droit d'obtenir une intervention humaine et de contester les décisions.

Le principal changement par rapport au RGPD consiste donc à limiter les restrictions imposées à la prise de décision automatisée aux décisions portant sur des catégories particulières de données à caractère personnel.

H- Transferts des données en dehors du Royaume-Uni – Tests d'adéquation (Section 25)

Le régime d'évaluation de l'adéquation des pays tiers a été réformé et rebaptisé "test de protection des données", qui met l'accent sur la prise de décision et les résultats fondés sur le risque.

Le test sera respecté si le niveau de protection des données n'est "pas matériellement inférieur" à celui prévu par le droit britannique.

Les facteurs suivants sont considérés comme pertinents :
- le respect de l'État de droit et des droits de l'homme ;
- l'existence et les pouvoirs d'une autorité chargée de la protection des données ;
- l'existence d'une autorité de protection des données et ses pouvoirs ;
- l'existence d'un mécanisme de recours judiciaire ou non judiciaire ;
- les règles concernant les transferts ultérieurs ;
- les obligations internationales pertinentes ;
- la constitution, les traditions et la culture.

Ces amendements offrent une plus grande flexibilité au gouvernement britannique lors de l'examen des décisions d'adéquation du Royaume-Uni.

En premier lieu, le seuil d'appréciation du niveau de protection des données dans le pays tiers qui consiste sous le régime actuel à évaluer si ce niveau est « essentiellement équivalent »[11] à celui conféré par la législation de l'Union européenne passe à une évaluation du niveau de protection des données qui ne doit pas être « matériellement inférieur » à celui prévu par la législation britannique. On ne peut pas pressentir à ce stade dans quelle mesure ce changement aura des implications sur les conclusions des futurs tests de protection des données.

En deuxième lieu, le nouveau test ne contiendra pas d'évaluation des lois et des pratiques des autorités du pays tiers, notamment des services de renseignement, en matière d'accès aux données personnelles. Ceci constitue une divergence majeure par rapport aux recommandations du Comité européen de la protection des données[12], à la suite de l'arrêt Schrems II de la Cour de Justice de l'Union européenne et par rapport à la méthodologie de la Commission européenne dans son évaluation de l'adéquation des pays tiers.

[redacted]

I- Transferts des données en dehors du Royaume-Uni – garanties appropriées (Section 25)

Selon le régime actuel applicable au Royaume-Uni, en l'absence de décision d'adéquation, d'autres mécanismes de transfert sont disponibles (article 46 du UK-GDPR). L'utilisation de tels mécanismes de transfert est conditionnée à la mise en œuvre de garanties appropriées.

Désormais, ces garanties seront déterminées par le responsable de traitement ou le sous-traitant agissant de manière «raisonnable et proportionnée» par référence aux critères du «test de protection des données».

Cette modification semble introduire une approche par le risque dans la réalisation des Analyses d'impact des transferts des données.

[11] Voir CEPD, Recommandations 02/2020 sur les garanties essentielles européennes pour les mesures de surveillance, disponibles ici

[12] Voir entre autres, CEPD, Recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE, , disponibles ici ; CEPD, Étude juridique sur l'accès des gouvernements aux données dans les pays tiers, disponible ici

J- Allégement des obligations des responsables de traitements et des sous-traitants (Sections 15 à 24)

Les références aux «mesures de sécurité techniques et organisationnelles appropriées» sont remplacées par les références aux «mesures appropriées, y compris les mesures techniques et organisationnelles». (Section 15)

Les responsables du traitement et les sous-traitants non établis au Royaume-Uni **n'auront plus l'obligation de désigner un représentant** du Royaume-Uni dans certaines circonstances. (Section 16)

Le projet de loi supprime l'obligation de désigner un délégué à la protection des données (DPD) (Section 17). À la place du DPD, les organisations seront tenues de nommer **une personne responsable de haut niveau** (« SRI – *Senior Responsible Individual* ») **s'ils sont un organisme public ou s'ils effectuent un traitement de données à caractère personnel qui, compte tenu de de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé** pour les droits et libertés des personnes (et pas seulement lorsque les activités du traitement impliquent un suivi régulier et systématique à grande échelle des personnes concernées ou lorsqu'elles consistent en un traitement à grande échelle de catégories particulières de données, comme c'est le cas actuellement avec le UK-GDPR).

Le SRI conservera bon nombre des caractéristiques du rôle et des tâches du DPD (Section 17).

La nouvelle loi vise à alléger les exigences de tenue du registre des traitements (Section 18)**. Désormais, seulement les RT et les ST qui effectuent des traitements à haut risque** auront l'obligation de conserver un nouveau type de registre qui contiendra des informations similaires à celles exigées par le RGPD.

Enfin, l'obligation de conduire une AIPD est remplacée par l'obligation de procéder à une «**évaluation du traitement à haut risque**» qui contient un résumé des finalités du traitement, une évaluation de la nécessité du traitement et des risques pour les individus et une description de la façon dont ces risques seront atténués (Section 20).

Les exigences de **consultation obligatoire préalable ont été supprimées** et remplacées par un processus de **consultation volontaire** (Section 21). La participation à une consultation volontaire sera considérée comme un facteur atténuant lors de toute enquête ou mesure d'application de la loi de l'ICO.

K- Modifications de la procédure d'élaboration et d'approbation des codes de bonnes pratiques (Section 22)

La loi instaure un nouveau processus d'élaboration des codes des bonnes pratiques.

Sur demande du Secrétaire d'État, l'ICO devra préparer des codes de bonnes pratiques de traitement des données. **Le Secrétaire d'État peut proposer des modifications à ces codes** que l'ICO devra prendre en compte afin de les intégrer dans le document final.
En cas de désaccord avec les modifications du Secrétaire d'État, l'ICO devra retirer le code.

Un groupe d'experts doit être désigné pour l'élaboration de chaque code et chaque code doit être accompagné d'une analyse d'impact.

L- Changement du rôle de l'ICO (Sections 29 à 35)

La loi introduit un ensemble d'objectifs et d'obligations stratégiques statutaires pour l'ICO :

- 2 objectifs principaux : (i) protéger les données en prenant en compte les intérêts des personnes concernées, des RT et l'intérêt général et (ii) promouvoir la confiance dans le traitement des données ;
- Le devoir de prendre en compte dans l'accomplissement de ses fonctions la « désirabilité de **la promotion de l'innovation et de la concurrence**», « l'importance de **la répression des crimes** » et « **la nécessité de la protection de la sécurité publique et la sécurité nationale** » ;
- L'ICO doit préparer sa stratégie et la revoir régulièrement ; Elle doit rendre compte de ses actions devant le Parlement ;
- L'ICO a l'obligation de consulter les autres régulateurs dont les domaines de compétence (compétition, économie, innovation) sont affectés par les décisions de l'ICO.

En déterminant les priorités stratégiques du gouvernement pour la protection des données, le secrétaire d'État détermine aussi les priorités stratégiques de l'ICO. Il doit les présenter devant le Parlement.

[redacted]

M- Gestion des plaintes (Sections 39, 40 et 45)

L'ICO pourra refuser une plainte, si la personne concernée n'a pas d'abord contacté le RT ou si le RT est encore en train de répondre à la plainte.

Le Secrétaire d'État pourra exiger qu'un RT communique à l'ICO le nombre des plaintes reçues dans une période spécifique

N- Gestion des cookies (Section 109)

Une nouvelle liste d'exemptions à l'obligation d'obtenir le consentement est établie, qui inclut l'utilisation de cookies (ou de technologies similaires) à des fins de:

- installation des mises à jour de sécurité nécessaires ;
- respect des préférences des utilisateurs ;
- collecte d'informations à des fins statistiques sur la façon dont le site Web/service est utilisé en vue d'apporter des améliorations.

IV- La réaction mitigée de l'Information Commissionner Office ICO

En résumé, après une première décision positive, John Edwards, actuel Commissaire de l'ICO et ancien Commissaire à la protection des données de Nouvelle-Zélande, a indiqué « avoir quelques inquiétudes ».

31 Mai 2023 - 1re réaction du Président de l'ICO :

> *"Je suis heureux que le gouvernement ait pris en compte mes préoccupations et qu'il ait apporté des modifications qui permettent au projet de loi de préserver notre indépendance réglementaire et de promouvoir la confiance dans le processus réglementaire. Cela signifie que le projet de loi sur le DPDI a évolué vers une position qui me permet de le soutenir pleinement"* [13].

18 Décembre 2023 : Mise à jour de l'avis de l'ICO

> « Je suis heureux de constater que le gouvernement a apporté certaines modifications au stade de la commission *de la Chambre des communes en réponse à mes commentaires, à savoir la définition des demandes vexatoires adressées à mon bureau et la rédaction des modifications des garanties pour le traitement à des fins de recherche. Toutefois, je constate que la majorité de mes commentaires n'ont pas encore été pris en compte, et je souhaiterais en particulier que le gouvernement prenne davantage en considération mon point de vue sur la définition du traitement à haut risque.*
>
> *Je suis satisfait des nouvelles propositions substantielles du gouvernement majoritaire et je salue :*
> - *D'autres changements visant à sauvegarder l'indépendance de l'ICO, à savoir la suppression de l'approbation par le secrétaire d'État des codes de pratique statutaires de l'ICO.*
> - *Les changements permettant à mon bureau de notifier par voie électronique les avis d'information, d'exécution et de sanction.*
> - *La disposition selon laquelle seul le traitement "nécessaire" aux fins de l'évaluation ou du recouvrement de l'impôt peut être considéré comme compatible en vertu de la nouvelle annexe relative au "traitement à considérer comme compatible avec la finalité initiale".*
> - *l'amendement visant à préciser que, lorsqu'elles répondent aux demandes d'accès des personnes concernées, les organisations ne doivent effectuer que des recherches raisonnables et proportionnées, ce qui reflète la position et les orientations actuelles de l'ICO.*

[13] ICO Response to the DPDI no 2 Bill, May 2023, disponible ici

- *L'extension de la période de signalement des violations de données à caractère personnel dans le cadre du PECR de 24 à 72 heures, afin de s'aligner sur le UK-GDPR, et l'extension de la période de signalement des violations de données à caractère personnel dans le cadre du GDPR.*

Dans l'ensemble, je soutiens le projet de loi, car il améliore l'efficacité du régime de protection des données au Royaume-Uni, défend les droits des personnes, apporte une certitude et une clarté réglementaires aux organisations et améliore la manière dont l'ICO réglemente. Toutefois, j'ai quelques inquiétudes concernant le pouvoir proposé d'exiger des informations à des fins de sécurité sociale ; en particulier, la mesure n'est actuellement pas assez étroitement définie dans la législation pour fournir les garanties appropriées. J'ai également fourni des commentaires techniques détaillés sur la manière dont je pense que les nouvelles clauses pourraient être améliorées afin d'apporter davantage de certitude et de clarté réglementaires à l'annexe 1, ainsi que des commentaires supplémentaires concernant les propositions en phase de prérapport à l'annexe 2. »[14]

V- La réaction de la Commission européenne

La Commission européenne suit de très près le sujet, d'autant plus que l'Union européenne demeure un partenaire commercial majeur du Royaume-Uni et que la Commission européenne, le 28 juin 2021, a adopté une décision d'adéquation au Règlement européen pour la protection des données personnelles (sur le terrain du UK GDPR). La décision reconnaît que le Royaume-Uni assure un niveau de protection adéquat en matière de données personnelles, pour une durée de 4 ans.

[redacted]

Conclusion

La France est le 5e partenaire commercial du Royaume-Uni, qui est son 6e client et son 8e fournisseur. En matière de services, le niveau des échanges s'est rétabli à son niveau pré-Brexit (32,5 milliards € en 2022, chiffres Direction générale du Trésor)
C'est dire l'importance de la loi en cours d'adoption pour l'avenir.

[14] Information Commissioner's Further Response to the Data Protection and Digital Information Bill (DPDI Bill), disponible ici

À titre indicatif, le nombre de plaintes, assez fluctuant, concernant des acteurs économiques français au Royaume-Uni s'élevait à :

- 24 en 2023,
- 49 en 2022,
- 26 en 2021,
- 39 en 2020,
- 41 en 2019,
- 26 en 2018.

La CNIL devra participer à l'analyse commune à réaliser au sein du CEPD sur le nouveau texte.

Ce dossier mérite ainsi d'être suivi de près et pourra faire l'objet, si vous en êtes d'accord, d'une mise à jour dans les mois à venir.