Note numéro 38
avril 2019

Note du CREOGN

Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale

PROTECTION DES DONNÉES ET CYBERSÉCURITÉ APRÈS LE BREXIT

ÉTAT DES LIEUX ET PERSPECTIVES

Par Philippe Aubert-Couturier, en stage Master 2 au CREOGN

Dans la suite de notre précédente Note sur le sujet[1], alors que l'hypothèse d'un *Brexit* sans accord se profile, les perspectives en matière de protection des données se dessinent peu à peu. Les interrogations sur ses relations avec l'UE au-delà se clarifiant, le passage du statut d'État membre à celui de pays tiers aura en effet de nombreuses conséquences sur les rapports qu'entretiendront les Britanniques avec leurs anciens partenaires. Le départ « sec » des Britanniques pourrait complexifier la donne pour les agences de sécurité britanniques, en termes d'échanges de données comme de coopération en matière de cybersécurité.

La nature des relations qu'entretiendra le Royaume-Uni avec ses partenaires européens dépendra avant tout de sa mise en conformité avec le Règlement général sur la protection des données (RGPD) qui pose aujourd'hui le cadre européen en terme de protection des données. Si l'*Information Commissioner's Office* (ICO), l'organisme britannique chargé de la protection des données, assure que le Royaume-Uni s'y est d'ores et déjà conformé[2], qu'en sera-t-il une fois le *Brexit* consommé ?

1. Le cadre du RGPD

Une application immédiate quasi complète

Le Règlement général sur la protection des données (RGPD), entré en vigueur le 25 mai 2018, a depuis été intégré dans l'ensemble des législations des États membres de l'Union européenne[3]. Au Royaume-Uni, il a été engagé par l'adoption du *Data Protection Act 2018*[4]. Cette loi a instauré un cadre similaire au RGPD pour le traitement des données à caractère personnel, en introduisant notamment de nouvelles infractions telles que la divulgation ou la vente de données obtenues sans consentement.

L'ICO, équivalent britannique de la Commission nationale de l'informatique et des libertés (CNIL), a indiqué récemment que les obligations issues du RGPD devraient conserver leur niveau d'exigence suite au départ de l'Union européenne[5]. De fait, la sortie du Royaume-Uni ne devrait donc pas transformer radicalement le paysage numérique européen. La loi britannique sur la protection des données ne serait pas non plus impactée par le *Brexit*, en cas d'accord de départ comme en cas de « *no-deal* ». En outre, l'ICO a indiqué que le gouvernement britannique envisageait certaines mesures afin que les transferts de données du Royaume-Uni vers les pays de l'Espace économique européen (EEE) puissent continuer sans interruption. Toutefois, un

1 VIALLE, Ludmila. Le Brexit et la protection des données. Note du CREOGN [en ligne], n° 28, octobre 2017. Disponible sur : https://www.gendarmerie.interieur.gouv.fr/crgn/Publications/Notes-du-CREOGN/Le-Brexit-et-la-protection-des-donnees

2 The Information Commissioner's response to the House of Commons Justice Committee consultation on the implications of Brexit for the justice system », *ICO*, 10 novembre 2016.

3 CNIL. La protection des données dans le monde [en ligne], 24 janvier 2019. Disponible sur : https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

4 http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

5 Brexit et RGPD : petit manuel de survie de l'ICO [en ligne]. Mathias Avocats, 28 janvier 2019Disponible sur : https://www.avocats-mathias.com/donnees-personnelles/brexit-rgpd

Brexit sans accord aurait probablement des conséquences à court terme sur les échanges de données avec le Royaume-Uni. Dans ce cas, la libre circulation des données à caractère personnel des pays de l'EEE vers le Royaume-Uni pourrait se trouver interrompue jusqu'à ce que la Commission européenne et le Royaume-Uni s'entendent sur les modalités d'hébergement de ces données. Une adaptation temporaire serait donc nécessaire pour les organismes de traitement de données britanniques et européens.

Des interrogations à long terme se posent également quant à la situation post-*Brexit* : si l'on sait que le RGPD s'appliquera aux opérateurs britanniques qui traitent des données de citoyens européens, qu'en sera-t-il par exemple de ceux ne traitant que de données de ressortissants britanniques ou non européens ?

Des incertitudes quant aux échanges de données à l'issue du *Brexit*

Différentes hypothèses de sortie se profilent aujourd'hui pour le Royaume-Uni :

- rejoindre l'Association européenne de libre-échange (AELE) : quitter l'UE pour rejoindre l'AELE obligerait le Royaume-Uni à se conformer au RGPD, puisque le marché intérieur est soumis à l'harmonisation de la protection des données. Cette option n'est cependant pas celle privilégiée par le gouvernement britannique, qui souhaite un accord sur mesure ;

- un partenariat sur mesure : c'est l'option défendue par la Première ministre britannique (plan « *Chequers* »), qui viserait à créer une zone de libre-échange permettant la circulation des biens et des capitaux, mais pas des services et personnes. La Cheffe de gouvernement déclarait ainsi : « *Nous recherchons un partenariat nouveau équitable entre une Grande-Bretagne mondiale, indépendante, autonome et nos amis et alliés de l'UE (...) Nous ne souhaitons pas adopter un modèle déjà existant pour d'autres pays* »[6]. Cette solution, à laquelle l'UE se montre pour le moment défavorable, n'obligerait pas nécessairement le Royaume-Uni à continuer à mettre en œuvre le RGPD ;

- créer un nouvel accord de libre-échange : c'est l'option privilégiée par Bruxelles, sur le modèle de l'Accord économique et commercial global liant l'UE et le Canada[7]. Un accord auquel Londres se montre peu favorable, le jugeant trop contraignant pour ses intérêts ;

- une sortie sans accord : c'est l'option qui semble aujourd'hui la plus probable, le Parlement britannique rejetant l'accord négocié par son gouvernement. Le Royaume-Uni deviendrait alors un simple pays tiers vis-à-vis de l'UE, et leurs relations seraient alors uniquement régies par les règles relatives aux transferts hors UE du RGPD[8]. Le gouvernement britannique pourrait ainsi élaborer une loi de protection des données plus souple pour les entreprises et donc plus attractive pour l'activité commerciale, afin de gagner en compétitivité. On notera, à titre d'exemple, que de très nombreux médias américains, comme *LA Times* ou *Chicago Tribune*, ont d'ores et déjà coupé l'accès à leurs sites depuis l'Europe[9], préférant se passer des utilisateurs européens plutôt que de s'exposer aux risques d'une amende en cas de non-respect du RGPD. En outre, le droit de la protection des données étant soumis à de fréquentes évolutions, les régimes légaux applicables dans le Royaume-Uni et dans le reste de l'UE sont susceptibles de diverger très vite.

---

6 COLLOMP, Florentin. Theresa May dit adieu au marché unique européen. *Le Figaro* [en ligne], 16 janvier 2017. Disponible sur : http://www.lefigaro.fr/international/2017/01/16/01003-20170116ARTFIG00388-theresa-may-nous-ne-garderons-pas-un-pied-dans-l-ue-et-un-pied-dehors.php

7 Qu'est-ce que le CETA et quelles seront ses conséquences ?, *Commission européenne* [en ligne], 16 février 2017. Disponible sur : http://ec.europa.eu/trade/policy/in-focus/ceta/ceta-explained/index_fr.htm

8 HURSTEL, Alric, KOUDOU, A'drill. Brexit : quel encadrement des transferts de données personnelles vers le Royaume-Uni ?, *Haas avocats* [en ligne], 28 février 2019. Disponible sur : http://info.haas-avocats.com/droit-digital/brexit-quel-encadrement-des-transferts-de-donn%C3%A9es-personnelles-vers-le-royaume-uni-

9 LAUSSON, Julien. Le RGPD fête ses trois mois et des centaines de médias américains bloquent les Européens. Numerama [en ligne], 25 août 2018. Disponible sur : https://www.numerama.com/politique/409677-le-rgpd-fete-ses-trois-mois-et-des-centaines-de-medias-americains-bloquent-les-europeens.html

L'avenir de l'ICO parmi les autorités de contrôle européennes

La question se pose également quant au devenir de l'ICO au sein du Comité européen de la protection des données (*European Data Protection Board* – EDPB). Cet organe indépendant réunit l'ensemble des autorités de surveillance et de régulation des États membres de l'UE et de l'Espace économique européen, afin d'assurer l'application cohérente du RGPD dans l'ensemble du territoire européen. À la date du *Brexit*, l'ICO ne pourra plus demeurer membre de droit de l'EDPB. Le gouvernement britannique assure cependant qu'il continuera d'œuvrer au maintien de relations étroites entre l'ICO et les autres autorités de surveillance de l'UE[10]. Il convient d'ores et déjà de s'interroger sur les formes que prendra cette nouvelle coopération.

Si la bonne application du RGPD par le Royaume-Uni apparaît peu préoccupante, celle du règlement *E-Privacy* l'est en revanche davantage.

2. Les enjeux du projet de règlement *E-Privacy*

Prévu pour entrer en vigueur fin 2019, le règlement *E-Privacy* viendra remplacer la directive 2002/58 du 12 juillet 2002 (directive vie privée et communications électroniques). Il a vocation à renforcer la protection de la vie privée de l'internaute, en encadrant davantage l'exploitation des métadonnées et des adresses IP. De fait, de nombreux sites ont recours à ces outils de traçage à des fins de profilage. Les évolutions apportées par *E-Privacy* inquiètent donc naturellement les opérateurs du marché numérique qui utilisent ces données. Une révision du texte a ainsi été réclamée par les représentants de l'industrie du numérique et par les éditeurs de presse, à travers une lettre ouverte à la Commission[11].

À l'instar du RGPD, le règlement *E-Privacy* doit en effet s'appliquer sur un large spectre territorial et concernera notamment les données des utilisateurs de l'UE traitées par des services extérieurs à l'UE. L'enjeu est donc conséquent pour les acteurs extérieurs, comme en témoignent les propos de la Chambre américaine de commerce auprès de l'UE[12], qui dénonçait un règlement jugé pénalisant pour l'innovation.

Même si le Règlement *E-Privacy* devait initialement entrer en vigueur en même temps que le RGPD, son application a été progressivement reportée, l'échéance envisagée étant actuellement octobre 2019, à l'issue des futures élections européennes. Le Royaume-Uni post *Brexit* ne sera plus tenu d'appliquer le Règlement *E-Privacy*. Dans ce cas, il est probable que des points de divergence surgissent avec l'UE, opérateurs britanniques et européens n'étant plus soumis aux mêmes contraintes, ce qui pourrait, à défaut d'accord, fragiliser la légalité des flux de données avec le Royaume-Uni.

En matière de protection de données, le *Brexit* entraîne également certaines incertitudes quant aux processus de coopération ente le Royaume-Uni et ses futurs partenaires européens.

3. La coopération en matière de cybersécurité

Une réorientation des axes de coopération britanniques

Quelles évolutions dans la coopération en matière de cyberdéfense peut-on envisager suite au *Brexit* ? La stratégie de sécurité nationale britannique repose actuellement sur trois piliers : ses relations privilégiées avec les États-Unis, sa qualité de membre de l'OTAN et son appartenance à l'UE. Comme pour tout État, la coopération internationale est de fait l'un des moyens essentiels de lutte contre la cybercriminalité et il convient de souligner que le Royaume-Uni a activement soutenu la mise en route de la stratégie européenne de cybersécurité.

---

10 *« ICO and the EDPB », Information Commissioner's Office,* 2019.
11 Lettre ouverte de 50 médias et organisations contre le projet européen ePrivacy, *Offremedia* [en ligne], mars 2018. Disponible sur : https://www.offremedia.com/lettre-ouverte-de-50-medias-et-organisations-contre-le-projet-europeen-eprivacy
12 BEKY, Ariane. ePrivacy : après le RGPD, le règlement « cookies » est mal digéré [en ligne], 29 mai 2018. Disponible sur : https://www.silicon.fr/eprivacy-rgpd-reglement-cookies-209979.html

Le *Brexit* aura pour conséquence d'éloigner le Royaume-Uni du pilier européen, l'exposant à être le maillon faible de l'édifice. Qu'en sera-t-il par exemple de la participation britannique aux exercices de cybersécurité menés en Europe ? L'exercice Cyber Europe, organisé par l'Agence européenne de cybersécurité (ENISA), développe ainsi régulièrement la coopération entre les États européens. Cyber Europe 2018 avait rassemblé 30 pays, dont le Royaume-Uni, autour d'une simulation de cyber-incidents de grande ampleur.

Le Royaume-Uni devra à l'avenir privilégier les relations bilatérales et renforcer son alliance avec le pilier américain. Dans sa coopération avec les États européens, il pourra peut-être davantage s'appuyer sur l'OTAN, et en particulier sur le Comité de cyberdéfense. Ce dernier maintient en effet une étroite collaboration avec l'UE, notamment en matière de partage d'informations relatives aux cybermenaces.

La directive NIS et la coopération européenne

La directive 2016/1148 du 6 juillet 2016[13], également appelée directive NIS (*Network Information Security*), vise à instaurer un niveau commun exigeant de sécurité des réseaux et des systèmes d'information, auquel chaque État membre doit se conformer. Tout opérateur de services essentiels ou fournisseur de services numériques opérant au sein de l'Union se doit de maintenir des niveaux élevés de sécurité et de résilience. Si le Royaume-Uni a, depuis 2016, transposé la directive, à travers la *Data Protection Act 2018*, des interrogations demeurent.

La directive NIS instaure notamment un système de coopération européen, fondé sur le signalement des incidents de sécurité dont sont victimes les opérateurs au sein de l'UE. Ce dispositif ne prévoit pour autant pas la coopération avec des États extérieurs. Dès lors, quelle relation avec le Royaume-Uni peut-on envisager ? La place des agences britanniques dans cette architecture demeure aujourd'hui inconnue, le risque étant qu'elles se retrouvent exclues du réseau de coopération européen. Suite au *Brexit*, les autorités britanniques pourraient donc avoir à affronter de nouvelles difficultés pour enquêter sur des actes de cybercriminalité et pour les réprimer. Une coopération internationale moins efficiente viendrait compliquer la lutte contre les opérations criminelles commises dans l'espace cyber.

Cela est d'autant plus important que les conséquences de l'application du RGPD pour mieux signaler la cybercriminalité sont d'ores et déjà visibles. Ainsi, en 2018, ce sont quelque 145 intrusions contre les établissements financiers britanniques qui ont été rapportées, contre seulement 25 en 2017[14], selon un rapport de la *Financial Conduct Authority*. Cette augmentation significative de signalements est due à l'obligation faite aux entreprises par le RGPD de signaler toute cyberattaque dans les 72 heures, sous peine de devoir s'acquitter de pénalités.

Conclusion

Des interrogations persistent donc concernant les transferts de données avec le Royaume-Uni, au moment de sa sortie effective de l'UE. Pour autant, l'application du RGPD par les Britanniques ne devrait pas être remise en cause, trop d'intérêts liant le Royaume-Uni et l'UE autour des questions de traitement des données à caractères personnel. En revanche, l'application de plusieurs autres réglementations s'avère plus incertaines.

Le *Brexit* inaugure également une période d'incertitudes quant aux relations de coopération en matière de cybersécurité qu'entretiendra le Royaume-Uni avec ses principaux partenaires européens. Un recentrage vers l'alliance Atlantique semble envisageable, ainsi qu'un renforcement des coopérations bilatérales.

Si de nombreux observateurs estiment que l'appartenance à l'UE renforce la sécurité intérieure des États, certains avancent au contraire que cette dernière relève essentiellement de logiques nationales, sur lesquelles l'UE n'a que peu d'effets. Quoi qu'il en soit, le *Brexit* permettra de mesurer les implications réelles du projet européen sur les enjeux de sécurité intérieure ainsi que sur les capacités de résilience des agences britanniques.

13 https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ:L:2016:194:TOC

14 Royaume-Uni : les cyberattaques contre les établissements financiers multipliées par 5 en 2018. *Les Échos*, février 2019.