Note numéro 28
octobre 2017

Note du CREOGN

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

LE BREXIT ET LA PROTECTION DES DONNÉES

Rédigée par Ludmilla VIALLE, stagiaire au CREOGN, étudiante à l'université Paris II Panthéon-Assas (2016-2017)

Longtemps caractérisé par sa liberté numérique, le Royaume-Uni a tardé à développer une protection juridique pour les données à caractère personnel. Si cette situation semblait a priori propice au développement des affaires, elle ne permettait pas pour autant de conférer aux entreprises nationales un gage de confiance, notamment lorsqu'elles se voyaient transférer des informations provenant d'un autre pays. C'est la raison pour laquelle, à la demande du secteur, l'État se dota dès 1984 d'une législation non-Orwellienne, relative à la protection des données. Le gain d'attractivité en résultant ne permit toutefois pas de résoudre les disparités territoriales. C'est pourquoi le gouvernement lança un programme d'inclusion numérique au cours de l'année 1990. De même, au niveau européen, la Commission envisagea la création d'une base juridique commune, capable d'instaurer un marché unique 2.0 plus uniforme et compétitif. Les négociations en découlant se heurtèrent à de nombreuses difficultés, au nombre desquelles figure l'opposition britannique à toute contrainte stricte.

Fort de cette harmonisation, le Royaume-Uni pèse aujourd'hui lourdement dans l'écosystème numérique. En se dotant, dès 2015, du plan d'action audacieux *TechNation,* il a su constituer un espace digital de près d'1,5 million d'experts, dont la performance lui vaut la 7e position au classement européen DESI (Digital Economy and Society Index[1]). Cette attractivité pourrait être encore améliorée par le Règlement Général de Protection des Données (RGPD), qui se substitue à l'ancienne directive 95/46/CE.

Toutefois, l'annonce du Brexit ouvre une période d'incertitude. Les négociations ouvertes le 19 juin 2017 attestent de cet état et vont opposer pendant les deux prochaines années David Davis, eurosceptique en charge de la représentation des intérêts britanniques, et Michel Barnier, fédéraliste aguerri agissant pour le compte de la Commission européenne.

Si cette quête souverainiste ne semble pas avoir d'impact sur le niveau actuel de protection des données, une interrogation se pose sur le long terme.

1. Un court terme certain : une harmonisation temporaire quasi complète

Jusqu'à la fin du processus de négociation, le Royaume-Uni demeure membre de l'Union européenne. Il est à ce titre assujetti à la mutation du marché unique numérique, tant d'un point de vue théorique que pratique.

L'appartenance à un marché unique numérique renforcé

- Un marché unique en mutation :

À partir des années 80, la communauté internationale s'est saisie des problématiques de flux

1. https://ec.europa.eu/digital-single-market/en/desi

transfrontaliers de données, au moyen de divers instruments normatifs[2]. L'Union européenne fait figure d'exception en élaborant une harmonisation plus approfondie, capable d'instaurer un marché unique numérique performant. C'est ainsi que le Royaume-Uni a transposé notamment les directives 95/46/CE et 2002/58/CE (vie privée et communication électronique). Pour assurer une bonne mise en œuvre de ces règles complexes et détaillées, la directive 95/46 prévoit, en plus de l'action normative classique de la Cour de Justice[3], la création du « G29 ». Ce groupe de travail est chargé d'analyser la régulation opérée dans différents États, à des fins de conseils et d'éventuelles propositions de projets de modification à la Commission[4]. En dépit de son activité intense, une étude comparative de la Commission de 2010 fait état de pratiques régulatrices nationales divergentes[5]. Sur le plan juridique, certaines notions ne font pas consensus. La législation autrichienne, par exemple, prévoit qu'il n'est pas possible d'identifier une personne à partir de « moyens légaux », tandis que la loi britannique retient le critère de probabilité. Sur le plan pratique, les autorités de régulation anglaise et irlandaise se livrent à une action disciplinaire plus clémente que leurs homologues européens, entraînant ainsi une concurrence conflictuelle[6].
Ces éléments, corrélés aux rapports DESI, font état d'une Europe à plusieurs vitesses, pour laquelle il devient impérieux d'approfondir l'harmonisation entreprise, notamment pour appréhender les nouveaux usages numériques.

- Un marché approfondi :

En poursuivant une nouvelle logique de conformité, le RGPD, dont l'application sera directe dès le 25 mai 2018, constitue la norme de référence en matière de protection des données personnelles[7]. Son rayonnement, d'abord continental, s'étend aux responsables de traitement de données (directs et indirects), établis sur l'espace économique européen, ainsi qu'aux services intéressant leur résidents. C'est la raison pour laquelle tout transfert de données vers l'extérieur nécessite une certaine euro-compatibilité. Il s'agit en effet de respecter les garanties des usagers du service numérique, d'ailleurs renforcées autour du droit à l'effacement des données concernant les mineurs, l'action collective, la réparation des dommages, ou encore la portabilité[8]. Toute violation de ce règlement fera l'objet de sanctions graduées, par les autorités nationales, puis européennes. Leurs pratiques devraient être davantage harmonisées par le Comité Européen de la Protection des Données, qui succède au G29. Une faible marge de manœuvre reste envisageable pour toute question de forme propre à l'organisation administrative ou à une certaine culture régalienne. Il est toutefois utile de préciser que cette uniformisation s'opère dans le respect des ordres juridiques internes des États membres. Par le biais de 56 renvois au droit national, le RGPD leur accorde en effet une certaine latitude. Il s'agit essentiellement d'appréhender les différentes organisations administratives et sensibilités sectorielles, pour garantir sa cohérence et sa compréhension[9].
La directive européenne Network Information Security (2016/1148) conforte ce règlement sous un aspect plus technique, en fixant un niveau commun élevé de sécurité des systèmes d'informations, auquel devront se conformer les États membres par le biais d'une stratégie nationale.
Ce corpus juridique devrait être prochainement renforcé par le projet de règlement e*Privacy*. Ce dernier

2. Nathalie MÉTALLINOS, « L'évolution du droit européen en matière de protection des données à caractère personnel et sa pénétration dans les droits nationaux : principes fondateurs et instruments de régulation », *L'Observateur de Bruxelles*, mars 2013, n° 93, p. 8-17.
3. Laraine LAUDATI, *Summaries of EU court decisions relating to data protection 2000-2015,* OLAF, 21 janvier 2016.
4. Jacob KOHNSTAMM, *14th and 16th reports on the article 29 working party on data protection, publications office of the European Union*, 2013 et 2015.
5. Commission Européenne, Direction Générale Justice Liberté et Sécurité : « Étude comparative sur les différentes approches des nouveaux défis en matière de protection de la vie privée, en particulier à la lumière des évolutions technologiques », rapport final du 20 juin 2010, [http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_fr.pdf].
6. Marc CHERKI, « Protection des données : la Cnil plus stricte que Bruxelles », *le Figaro*, 12 octobre 2012.
7. Jérôme LAGASSE, « Le règlement général de protection des données, vers une grande charte des libertés de l'identité numérique ? », *Note du CREOGN n°22*, mars 2017[https://www.gendarmerie.interieur.gouv.fr/crgn/Publications/Notes-du-CREOGN/Le-Reglement-general-de-protection-des-donnees-vers-une-grande-charte-des-libertes-de-l-identite-numerique].
8. Dans une optique économique, la Commission européenne envisage par ailleurs une extension de cette circulation sous le prisme de la propriété des données non personnelles : voir en ce sens l'avis du Conseil National du Numérique, *La libre circulation des données dans l'Union européenne*, avril 2017.
9. Cela soulève une interrogation conceptuelle sur la mixité du Règlement : l'article 288 du Traité sur le Fonctionnement de l'Union européenne dispose en effet que : « Le règlement a une portée générale. Il est obligatoire dans tous ses éléments et il est directement applicable dans tout État membre. La directive lie tout État membre destinataire quant au résultat à atteindre, tout en laissant aux instances nationales la compétence quant à la forme et aux moyens. La décision est obligatoire dans tous ses éléments pour les destinataires qu'elle désigne. Les recommandations et avis ne lient pas ».

vise en effet à remplacer la directive 2002/58 par des dispositifs capables d'appréhender les nouveaux usages numériques des internautes, dans un cadre plus respectueux de leur vie privée.
Enfin, s'agissant des données non personnelles, les États membres pourront, à leur convenance, ratifier la directive 2016/943 relative au secret des affaires, afin de protéger plus abondamment les entreprises contre l'espionnage.

L'implication britannique dans le marché unique numérique

Le Royaume-Uni doit s'engager sérieusement dans la transition numérique, d'abord parce que son implication européenne donnera le ton des relations postérieures avec l'Union, ensuite, pour satisfaire le lobby digital, fortement attaché à l'existence d'une régulation adéquate. Pour ce faire, le gouvernement a mené une évaluation de ses politiques publiques numériques, dont le rapport, publié le 21 décembre 2016, faisait état de la nécessité de mieux appréhender la gestion des risques cybernétiques. Il a par là même manifesté son intention de mettre en œuvre le futur RGPD[10] et la directive NIS (Network Information Security). Son engagement est conforté par l'action de l'*Information Commissioner's Office* (autorité régulatrice équivalente à la CNIL), qui publie de nombreux guides et conseils pour les professionnels concernés.

Toutefois, certaines questions pratiques restent en suspens. Si la directive NIS prévoit l'instauration d'un système de coopération entre les États membres, capable de gérer les « cyber-insécurités » rencontrées par les opérateurs numériques, elle n'envisage pas pour autant d'éventuelles participations extérieures. Quid de la position du Royaume-Uni, en cas de sortie de l'Union, et plus largement de l'espace économique européen ? De plus, l'exécutif britannique ne s'est pas encore prononcé sur la transposition à venir des directives *ePrivacy* et « secrets des affaires ». S'il devait respecter ses obligations européennes, pendant le processus de sortie, sa position ultérieure reste pour autant incertaine.

2. Un long terme incertain : une attractivité priorisée

Si aucun doute ne subsiste quant au champ d'application du RGPD, rien n'indique que le Royaume-Uni maintiendra, après sa sortie, un niveau de protection équivalent pour les citoyens non-européens. Il pourrait ainsi développer, de manière stratégique, une « attractivité data » communément acceptable.

Les différentes options « data » du Brexit

L'application du RGPD pourrait être poursuivie, si le Royaume-Uni décidait de se maintenir dans l'Union - ce qui reste théoriquement envisageable -, mais également en cas d'adoption de l'accord portant sur l'Espace Économique Européen, à l'instar de la Norvège. Cela permettrait de conserver un certain accès au marché tout en diminuant les contributions budgétaires. Toutefois, aucun contrôle migratoire ne serait admis et l'influence britannique sur les politiques communautaires serait limitée.
D'autres formes de partenariats plus ténues pourraient être envisagées. Une adhésion à l'Association Européenne de Libre Échange, analogue au modèle suisse, permettrait de disposer d'un accès gratuit au marché. Agrémenté d'un traité relatif à la protection des données compatible avec le RGPD, le secteur numérique n'en serait que peu affecté. Pour autant, cette hypothèse semble inadéquate, car elle entraînerait une exclusion de la libre circulation des services financiers, ainsi qu'une impossibilité de restreindre les flux migratoires européens, accompagnée d'une participation budgétaire atténuée. L'Accord Économique et Commercial Global, liant l'UE et le Canada, constitue en revanche un précédent plus pertinent. Il implique un accès au marché unique, par le biais de tarifs préférentiels et de subventions de péréquation. Un traité « data compatible » devrait également être adopté entre le Royaume-Uni et l'Union européenne. Ce serait également le cas si Londres et Bruxelles ne parvenaient pas à s'entendre. Le « *privacy Shield* » et les standards ISO offrent alors des illustrations pertinentes. Quoi qu'il en soit, le Brexit ne présente aucune option parfaite et nécessite des compromis.

10. https://www.gov.uk/government/consultations/general-data-protection-regulation-call-for-views

Vers un dumping régulateur communément acceptable ?

Pour le Royaume-Uni, le Brexit renvoie avant tout à une quête souverainiste. Pour preuve, les arguments de campagne des « *brexiters* », qui ont prévalu lors du référendum en date du 23 juin 2016 avec près de 51,9 % des voix, font état de la nécessité d'établir un nouvel espace de libre échange, exempt de toutes contraintes budgétaires et réglementaires, tel que peut l'être l'impossible contrôle migratoire. L'hypothèse du maintien du Royaume-Uni apparaît en pratique peu probable. Il reste alors à poursuivre le processus de sortie, dans un contexte agité. L'objectif serait en effet de parvenir à un juste équilibre entre une perte de gouvernance internationale et la mise en place d'un espace économique plus libéral. Pour autant, le Royaume-Uni n'envisage aucunement de se positionner en ermite sur la scène internationale. Du fait de sa dépendance au marché unique, il entretiendra certainement une relation économique avec l'Union, mais de manière plus ténue et ouverte sur l'extérieur. Il reste à savoir dans quel contexte il pourra négocier.

L'Union européenne se positionne, à l'inverse, de manière plus éclairée et organisée, parce qu'au-delà d'une désunion apparente, elle perçoit davantage l'opportunité de se renouveler autour d'un projet plus approprié pour chacune des parties, évitant ainsi les entraves qu'elles ont connues. Pour ce faire, les 27 ont convenu de grandes orientations visant à guider Michel Barnier dans la négociation. Elles devront d'abord se concentrer sur les modalités pratiques de rupture, avant d'envisager une relation économique constructive. Cela permettra également d'éviter tout risque « d'Europe à la carte », dont pourrait bénéficier injustement le Royaume-Uni, en procédant notamment à un maintien sur le marché accompagné d'une politique de gestion migratoire et de dumping. Dans cette optique, les modèles suisse et canadien paraîtraient pertinents, à commencer par le plan économique.

L'économie britannique semble résister aux pronostics désastreux formulés par de nombreux économistes. Si cela s'explique par une certaine stabilité de la consommation des ménages, la situation particulière du secteur numérique est en revanche plus complexe. Contrariés, certains experts, tel que Stephen Hawking, s'alarment de ce « désastre » qui affecterait le marché numérique et la libre circulation des spécialistes, encore que la migration choisie reste envisageable. De plus, la perspective du Brexit interroge sur le futur niveau de protection des données. C'est pourquoi certaines entreprises soucieuses d'une réglementation stricte, telles que General Electric ou Sup, envisagent de fermer des établissements, à l'inverse de Google et Facebook, plus attirés par une souplesse éventuelle et par la conquête de nouveaux marchés sur un territoire disposant d'une culture similaire et d'une connexion à l'Europe. L'abandon futur du RGPD au profit d'une réglementation plus souple conférerait un cadre plus adapté et dynamique aux petites entreprises. Son euro-compatibilité contribuerait par la même à une certaine harmonisation de la régulation disciplinaire. Un tel cadre de protection, constaté par une décision d'adéquation de la Commission, permettrait le transfert de données vers ce nouvel État tiers[11], et contribuerait à la stabilité du secteur. Cette hypothèse semble corroborée par la position actuelle du Royaume-Uni, qui souhaite négocier un accord EU-UK sur la protection des données à caractère personnel[12].

Conclusion

Qu'il soit « *soft »* ou « *hard »*, le Brexit n'aura vraisemblablement que peu de conséquences en termes de protection des données. Cette dernière devrait ainsi relever du RGPD, ou tout du moins d'un niveau comparable pour les citoyens non européens. Il s'agit avant tout d'une quête souverainiste menée par le Royaume-Uni, dont le cap et la portée demeurent indéterminés. Comme l'écrivait La Bruyère dans « Les caractères », «Tels se laissent gouverner jusqu'à un certain point, qui au-delà sont intraitables et ne se gouvernent plus : on perd tout à coup la route de leur cœur et de leur esprit ; ni hauteur ni souplesse, ni force ni industrie ne les peuvent dompter ; avec cette différence que quelques-uns sont ainsi faits par raison et avec fondement, et quelques autres par tempérament et par humeur ».

11. Transfert fondé sur une décision d'adéquation - Article 45 du RGPD.
12. Michael GUILLOUX, « Brexit : le gouvernement britannique demande un accord UE-UK sur l'échange et la protection des données personnelles avant sa sortie de l'Union », 26 août 2017 [https://www.developpez.com/actu/157101/Brexit-le-gouvernement-britannique-demande-un-accord-UE-UK-sur-l-echange-et-la-protection-des-donnees-personnelles-avant-sa-sortie-de-l-Union/].