L'impact du Brexit sur la protection des données à caractère personnel. Entre Charybde et Scylla.

Christina Koumpli

L'impact du Brexit sur la protection des données à caractère personnel

Entre Charybde et Scylla

Christina Koumpli

Maître de conférences en droit public, Avignon Université, LBNC

Tenter de déterminer l'impact du Brexit sur la protection des données à caractère personnel revient en réalité à répondre à la question de savoir si le droit peut s'imposer à la puissance des faits ou bien si, au contraire, ce sont les faits qui font le droit ou appellent le droit à les légitimer.

Ces faits à l'égard du Brexit sont de différents ordres et méritent d'être mis en lumière au regard des projets de décision d'adéquation de la Commission européenne publiés le 19 février 2021 ; l'une au titre du règlement général sur la protection des données (RGPD)[1] et l'autre au titre de la Directive « Police Justice »[2,3].

Tout d'abord, le Royaume-Uni ayant été un membre de l'Union européenne (UE) jusqu'à très récemment (jusqu'au 31 janvier 2020), on peut penser qu'il existe la présomption d'un ordre juridique britannique prévoyant une protection « essentiellement équivalente » à celle de l'UE, critère substantiel d'évaluation du niveau d'adéquation de la législation des pays tiers d'après la récente jurisprudence *Schrems II* de la Cour de justice de l'Union européenne (CJUE) de 2020[4]. De plus, étant donné que la dernière norme adoptée en la matière au niveau européen avant la sortie du Royaume-Uni de l'UE était un règlement, la marge de manœuvre du Parlement britannique est un principe très faible. Ce constat pourrait permettre d'affirmer, avec une certaine certitude, qu'avant comme après le Brexit les citoyens britanniques bénéficient d'une protection « identique » à celle dont jouissent les citoyens européens. Dès lors, ces derniers ne devraient en principe n'avoir rien à craindre du Brexit à l'égard de la protection de leurs données personnelles transitant par le Royaume-Uni.

Cependant, un autre fait intéressant à relever est que le Royaume-Uni, en quittant l'UE, est devenu en vertu du RGPD un État tiers avec lequel les transferts de données personnelles sont en principe *interdits* étant donné que tout État tiers à l'UE est supposé ne pas garantir un niveau de protection aussi élevé que cette dernière vis-à-vis de ces citoyens. Ce « bouclier européen » de protection des données est une « marque de fabrique de l'UE », l'une des conditions de la réussite de l'intégration européenne et une composante des règles de concrétisation du droit fondamental garanti par l'article 8 de la Charte des droits fondamentaux de l'UE.

---

[1] European Commission, *Draft Implementing decision pursuant Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom*, 19th February, 2021, 88p.

[2] European Commission, *Draft Implementing decision pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom*,19th February, 2021, 51 p.

[3] L'article fait état du droit en vigueur au jour du colloque et lorsque les deux décisions d'adéquation n'avaient pas encore été adoptées, celles-ci ayant été prises le 28 juin 2021. Par ailleurs, la présente contribution traite essentiellement du projet de décision d'adéquation au regard du RGPD. Lorsqu'il est fait référence au projet de décision d'adéquation relative à la directive en matière de protection des données dans le domaine répressif, cela sera explicitement indiqué.

[4] CJUE, 16 juillet 2020, *Data Protection Commissioner c/ Maximilian Schrems et Facebook Ireland*, aff. C-311-18 – « Schrems II».

Cette interdiction peut néanmoins être levée de façon dérogatoire en employant les procédés suivants : une décision d'adéquation ; des clauses contractuelles types ; des règles d'entreprises contraignantes (BCR) ; des certifications ; des codes de conduite ; d'autres dérogations prévues par le RGPD (consentement explicite, exécution d'un contrat, etc.).

Ainsi, il existe bien une barrière au libre transfert de données personnelles imposée par le droit de l'UE mais ces possibilités de dérogation révèlent la fiction d'un espace européen hautement protecteur de ces données.

De telles solutions juridiques légitimant les transferts de données vers des États tiers peuvent avoir des conséquences si importantes en termes de droits et de libertés qu'elles doivent être employées avec une grande prudence, ce qui implique *le caractère exceptionnel* de leur application avec une appréciation très stricte des critères de leur mise en œuvre, une faible marge de manœuvre et l'inacceptabilité d'une quelconque transgression des droits des citoyens européens[5].

En revanche, à l'opposé de ces possibilités de transferts qui entraînent des risques juridiques, la décision d'adéquation est en quelque sorte une « décision miracle » dans la mesure où une fois adoptée par la Commission européenne, elle étend fictivement le territoire protecteur des données personnelles à des pays tiers et permet ainsi des transferts de données libres de toute autre formalité. La seule condition pour qu'une décision d'adéquation soit adoptée est la présence d'un niveau équivalent (devenue « substantiellement équivalent » après la jurisprudence *Schrems II* précitée, un niveau d'exigence plus élevé que lorsque l'exigence était une simple « équivalence »)[6].

Pour ce qui est de l'appréciation des règles limitant l'accès aux données personnelles pour raison de sécurité nationale et afin de limiter les ingérences dans les droits fondamentaux, le WP254[7] prévoit les conditions suivantes :

1) le traitement doit reposer sur des règles claires, précises et accessibles (base juridique) ;

2) la nécessité et la proportionnalité au regard des objectifs légitimes poursuivis doivent être démontrées ;

3) le traitement doit faire l'objet d'un contrôle indépendant ;

4) les particuliers doivent disposer de voies de recours effectives.

---

[5] C. KOUMPLI, *Les données personnelles sensibles : une contribution à la protection du droit fondamental à la protection des données à caractère personnel. Étude comparée : Union européenne, Allemagne, France, Grèce, Royaume-Uni*, thèse de doctorat soutenue le 18 janvier 2019, Université Paris I [à paraître chez Editions Pedone en 2022], pp. 475-489, spéc. pp.476-477

[6] Pour que ce niveau soit constaté, la Commission dispose d'un référentiel avec le WP254 qui contient une grille d'évaluation divisée en deux grandes parties. D'une part, il s'agit d'apprécier l'existence de principes généraux en matière de protection des données dans la législation nationale de l'État tiers (notions, fondements du traitement loyal et licite pour des finalités légitimes, principe de limitation de la finalité, principe de qualité et de proportionnalité des données, principe de conservation des données, sécurité et confidentialité, transparence, droit d'accès, de rectification, d'effacement, et d'opposition, restrictions concernant les transferts ultérieurs, règles relatives aux données sensibles, au démarchage, au profilage et à la décision automatisée). D'autre part, sont évalués les mécanismes procéduraux qui permettent une réelle effectivité de la protection. Précisément, sont examinées les règles garantissant l'indépendance de l'autorité, l'existence de sanctions effectives, les obligations de rendre compte des responsables de traitements, la possibilité que les personnes puissent effectivement exercer leurs droits et l'existence de mécanismes de recours appropriés.

[7] Groupe de travail de « Article « 29 » sur la protection des données, *Critères de référence pour l'adéquation*, Adoptés le 28 novembre 2017, Version révisée et adoptée le 6 février 2018, WP 254 rev.01, 18/FR, 10 p.

Un troisième fait à mentionner est l'importance du « coût de l'inadéquation » de l'ordre juridique britannique. Bien que cet élément ne soit pas juridique et qu'il ne constitue pas un critère de la grille d'évaluation du niveau adéquat du droit d'un pays tiers, il convient cependant de relever qu'une étude récente[8] estime ce coût à environ entre 1. 116€ et 1.7856€ milliards d'euros pour les entreprises britanniques. De plus, les mécanismes à disposition sans décision d'adéquation (CCT, BCR, etc.) présentent difficilement une alternative fiable puisque leur champ d'application est étroit et ils souffrent d'une immaturité juridique partielle [9], comme le rapporte le Parlement européen dans un riche rapport publié en avril 2021. La décision d'adéquation semble donc non seulement être un « parapluie juridique » plus large mais surtout une solution plus intéressante financièrement. En outre, il convient de souligner que ce coût ne prend pas en compte l'impact économique de la réduction des échanges commerciaux entre l'UE et le Royaume-Uni, la réduction des investissements au Royaume-Uni, ou encore la délocalisation des entreprises hors UE, comme le souligne un chercheur du *UCL European Institute* dans un rapport écrit déposé au Parlement britannique[10].

Cet argument, bien qu'il soit secondaire lorsqu'on se préoccupe de déterminer le niveau substantiellement équivalent du droit du Royaume-Uni à l'égard du cadre juridique de l'UE, semble orienter en filigrane les évolutions juridiques en la matière.

Il y a également un coût pour l'UE qui ne se mesure pas seulement en termes financiers ; il s'évalue aussi en termes de politique mondiale de l'UE puisque cette dernière vise à exporter son modèle de protection des données personnelles afin de s'imposer comme une figure humaniste du marché numérique mondial et du développement de la société connectée de demain.

Ainsi, bien que l'ordre juridique britannique présente de réelles défaillances en termes de protection des données personnelles alors qu'il était jusqu'à récemment un État membre de l'UE[11], la Commission européenne a publié le 19 février 2021 un projet de décision très long déclarant le droit britannique substantiellement équivalent au cadre juridique européen (RGPD).

Telle est la toile de fond à partir de laquelle il s'agit d'apprécier l'impact du Brexit sur la protection des données à caractère personnel.

Il conviendra ainsi, dans un premier temps, d'exposer plusieurs éléments permettant *a priori* de rassurer autant les citoyens britanniques que les citoyens européens dont les données seront traitées, transférées ou transiteront par le Royaume-Uni.

Néanmoins, il importera par la suite de démontrer en quoi cette apparente garantie, qui paraît rassurante, est trompeuse.

En effet, il nous semble que cet impact, en apparence inexistant ou minime, est en réalité très important au regard du niveau de protection des données personnelles assurée par l'ordre juridique britannique mais surtout en tant que révélateur d'incohérences profondes du système européen de protection de ce type de données.

---

[8] D. MCCANN *et al.*, "The cost of data inadequacy", *New Economics Foundation*, 23 November 2020.

[9] « At the time of writing, the remaining mechanisms hardly present a reliable alternative, since they are encumbered by similar concerns to a UK adequacy decision and are partially immature, as well as narrow in scope. », in European Parliament, *EU-UK private-sector data flows after Brexit, Settling adequacy*, EPRS, April 2021, p. 1

[10] Source : https://committees.parliament.uk/writtenevidence/7972/default/

[11] Ce qui a été souligné par le Parlement européen, par le Comité Européen de Protection des Données (l'ex-Groupe de l'article 29) appelé désormais EDPB ainsi que par la doctrine.

Dès lors, choisir entre une décision d'adéquation et d'autres solutions juridiques dérogatoires de transferts prévues par le RGPD conduit l'UE à choisir entre Charybde et Scylla, les deux monstres marins qui se sont présentés à Ulysse lors de son retour à Ithaque.

I. Un impact en apparence relatif

L'impact du Brexit en termes de protection des données personnelles semble relatif en ce sens qu'à la lecture du droit positif actuel et en cours d'adoption, les droits des personnes (à la fois européens et britanniques) paraissent garantis au regard des trois points suivants :

- en termes de niveau de protection des données localisées au Royaume-Uni à la fois pendant la période de transition (du 1er février 2020 au 31 décembre 2020) et à la suite de celle-ci, on pourrait être rassurés par le fait que la législation nationale britannique est issue d'une transposition de la réglementation européenne en la matière du fait de sa nature de membre jusqu'à très récemment, ce qui permet de présumer des divergences minimes entre les deux ordres juridiques (1) ;
- s'agissant de la période de transition, tout a été prévu pour que le niveau de protection ne recule pas lors de transferts de données (2) ;
- c) enfin, concernant les transferts de données réalisés après la période de transition, les inquiétudes pourraient être également écartées si l'on se fie au projet de décision d'adéquation de la Commission européenne publié en février 2021 qui après une minutieuse analyse a constaté que l'ordre juridique britannique est « substantiellement équivalent » aux standards européens (3).

L'impact du Brexit serait donc relatif à la lumière de tels arguments qui supposent que le niveau de protection des données personnelles accordée par le droit britannique est identique avant et après la sortie du Royaume-Uni de l'UE.

1. Une loi britannique « RGPD-compatible » et protectrice des données à caractère personnel

S'agissant du premier point mentionné, indépendamment des mesures qui seront prises dans les prochains mois (décision d'adéquation ou autres instruments prévus par le RGPD pour légaliser les transferts de données), une chose est certaine : le cadre juridique britannique relatif à la protection des données personnelles est dans une large mesure proche de celui de l'UE.

Ce cadre est composé des textes juridiques suivants :

- Le *UK GDPR* ou « RGPD du Royaume-Uni » qui a transposé dans l'ordre juridique britannique le RGPD en vertu du « droit retenu » prévu par la section 3 du *European Union Withdrawal Act 2019* tel que modifié par la *Data protection, privacy and Electronic Communications Regulation 2019*, qui inclut notamment les considérants du RGPD[12] ;
- la loi sur la protection des données de 2018 (*Data Protection Act 2018*, ci-après « DPA 2018 »), telle que modifiée par la *Data protection, privacy and Electronic Communications Regulation 2019* ;

[12] Le "*Explanatory Notes to the European Union (Withdrawal) Act 2018*" précise: "Where legislation is converted under this Section, it is the text of the legislation itself which will form part of domestic legislation. This will include the full text of any EU instrument (including its recitals)", paragraphe 83.

- l'*Investigatory Powers Act* (ci-après « IPA 2016 »).

Une convergence générale entre les deux cadres juridiques a effectivement été soulignée par la Commission européenne - dans ses projets de décisions d'adéquation au RGPD et à la Directive 2016/680[13] publiés le 19 février 2021[14] qui ont admis l'adéquation - ; cependant autant le Comité européen de la protection des données (CEPD ou European Data Protection Board - EDPB)[15] que le Parlement européen ont mis en question cette position.

En effet, en émettant certaines critiques, le CEPD a pu souligner que : « Le Royaume-Uni était jusqu'à récemment un État membre de l'UE ; par conséquent, en analysant sa législation et ses pratiques, l'EDPB a identifié de nombreux aspects comme étant essentiellement équivalents » (cons. 9). Avant de préciser que : « Le cadre de protection des données du Royaume-Uni s'inspire largement du cadre de protection des données de l'UE (en particulier le GDPR et la LED), ce qui découle du fait que le Royaume-Uni était un État membre de l'UE jusqu'au 31 janvier 2020. En outre, la loi britannique sur la protection des données de 2018, qui est entrée en vigueur le 23 mai 2018 et a abrogé la loi britannique sur la protection des données de 1998, précise davantage l'application du GDPR en droit britannique, en plus de transposer la directive [Police-Justice 680/2018] de l'UE, ainsi que d'accorder des pouvoirs et d'imposer des devoirs à l'autorité nationale de contrôle de la protection des données, l'ICO britannique » (cons. 38)[16].

Puis, il est affirmé plus loin que : « L'EDPB reconnaît que le Royaume-Uni a repris, pour l'essentiel, le chapitre V du GDPR dans le GDPR britannique (articles 44 à 49) et dans la DPA 2018 » (« *The EDPB recognises that the UK* ***has mirrored, for the most part****, Chapter V GDPR in te UK GDPR* »).

Ces réflexions conduisent finalement le CEPD à constater, à l'instar de la Commission européenne[17], que de nombreux principes (« *content principles* ») sont alignés sur ceux du GDPR et offrent donc un niveau de protection essentiellement équivalent à celui de l'UE. Parmi ces principes, on peut par exemple mentionner les concepts (par exemple, « données à caractère personnel », « traitement de données à caractère personnel », « responsable de traitement »), les motifs de traitement licite et loyal à des fins légitimes, la limitation de leur finalité, la qualité et la proportionnalité des données, la conservation des données, la sécurité et la confidentialité, la transparence, les catégories particulières de données, le marketing

[13] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes aux fins de la prévention, des enquêtes, de la détection ou des poursuites pénales les infractions ou l'exécution de sanctions pénales, ainsi que sur la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

[14] *op.cit.* (European Commission, *Draft Implementing…)*

[15] Le Comité Européen de la Protection des Données (en anglais EDPB) est un organe européen indépendant qui contribue à l'application cohérente des règles en matière de protection des données au sein de l'Union européenne et encourage la coopération entre autorités de l'UE chargées de la protection des données. Ce comité se compose de représentants des autorités nationales chargées de la protection des données et du Contrôleur européen de la protection des données. S'ajoutent les autorités de contrôle des États de l'AELE-EEE en ce qui concerne les questions liées au RGPD, mais sans droit de vote et sans possibilité de se présenter aux élections pour la présidence ou vice-présidence. L'EDPB a été institué par le RGPD et son siège se situe à Bruxelles. La Commission européenne et - pour ce qui est des questions liées au RGPD - l'Autorité de surveillance AELE ont le droit de participer aux activités et réunions du comité sans droit de vote.

[16] EDPB, *Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom*, pp. 10-11.

[17] European Commission, *Draft Implementing decision pursuant Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom*, 19th February, 2021.

direct, la prise de décision automatisée, ou encore le profilage.

Le CEPD a également noté que le GDPR britannique et la DPA 2018 incluent des principes dont le contenu va plus loin que ce qu'exige le référentiel d'adéquation, un fait qui suggère un niveau de protection élevé de protection au Royaume-Uni. Il s'agit, par exemple, des principes liés aux notifications de violation de données personnelles, au délégué à la protection des données, aux évaluations d'impact sur la protection des données, ou encore à la protection des données par conception (*privacy by design*) et par défaut (*privacy by default*).

2. La période transitoire protectrice des transferts de données

La nécessité de ne pas entraver la libre circulation des données personnelles entre l'UE et le Royaume-Uni s'accompagne de celle de conserver un niveau de protection suffisant afin de n'impacter ni les droits des personnes résidant au Royaume-Uni ou résidant dans les États membres de l'UE, ni les obligations des entreprises britanniques ou européennes en termes de conformité au RGPD.

Ainsi, la protection des données personnelles a bénéficié de deux « périodes de grâce » depuis le Brexit. La première a été celle d'une période de transition générale du 1er février 2020 au 31 décembre 2020. En effet, aux termes du *Withdrawal Agreement* (accord de retrait), le Royaume-Uni a continué à être considéré provisoirement comme un État membre de l'UE et en ce sens, autant le RGPD que le droit primaire, mais aussi la jurisprudence de la CJUE en matière de protection des données personnelles, lui étaient applicables.

Cette situation a été prolongée par une seconde « période de grâce » selon le *Trade and Cooperation Agreement*[18], allant du 1er janvier 2021 au 30 juin 2021[19].

Dans l'attente d'une solution pérenne, telle qu'une décision d'adéquation, les données personnelles bénéficient jusqu'au 1er juillet 2021 d'une protection issue des dispositions de l'accord de commerce et de coopération entre l'UE et le Royaume-Uni.

En effet, aux termes de ce long document, il est notamment prévu :

« Article COMPROV.10 : Protection des données à caractère personnel

> 1. Les parties affirment leur engagement à assurer un niveau élevé de protection des données personnelles. Elles s'efforcent de travailler ensemble pour promouvoir des normes internationales élevées.

Article FINPROV.10A : Disposition provisoire pour la transmission de données à caractère personnel au Royaume-Uni

> 1. Pendant la durée de la période spécifiée, la transmission de données à caractère personnel de l'Union au Royaume-Uni n'est pas considérée comme un transfert vers

[18] *Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part*, JOUE L 149/10, 30. 4. 2021

[19] Article FINPROV.10A.

4. The "specified period" begins on the date of entry into force of this Agreement and, subject to paragraph 5, ends: (a) on the date on which adequacy decisions in relation to the UK are adopted by the European Commission under Article 36(3) of Directive (EU) 2016/680 and under Article 45(3) of Regulation (EU) 2016/679, or (b) on the date four months after the specified period begins, which period shall be extended by two further months unless one of the Parties objects; whichever is earlier.

> un pays tiers en vertu du droit de l'Union, à condition que la législation sur la protection des données du Royaume-Uni au 31 décembre 2020 (…) ».

Concrètement, ces dispositions impliquent qu'aucune autre formalité additionnelle ne devrait en principe être mise en place par les entreprises et organismes publics jusqu'au 1er juillet 2021. Ces organismes doivent toutefois respecter les principes généraux du RGPD (licéité, information des personnes concernées, droit de rectification, etc.). Les personnes ont donc pu bénéficier de droits et de recours, comme si le Royaume-Uni était encore un État membre de l'UE, jusqu'au 30 juin 2021.

Il convient également de souligner qu'afin de mieux garantir les droits des individus pendant cette période transitoire, l'UE a imposé au Royaume-Uni l'interdiction de modifier la législation nationale pendant la durée spécifiée par l'Accord. À défaut, il a été prévu que ce dernier prenait automatiquement fin (Article FINPROV.10A, §5).

Dès lors, on peut considérer que la continuité de la protection des données personnelles des Européens dont les données sont traitées ou transférées au Royaume-Uni constituait l'une des préoccupations du Brexit et des dispositions juridiquement contraignantes adoptées par les deux parties.

3. Le projet de décision favorable à l'adéquation de la législation britannique

Le 19 février 2021, la Commission européenne, faisant usage des pouvoirs qui lui sont conférés par l'article 45, paragraphe 3 du RGPD, a publié deux projets de décision d'adéquation de la protection des données à caractère personnel assurée par le Royaume-Uni : l'un en application du RGPD ; l'autre en vertu de la directive en matière de protection des données dans le domaine répressif.

Précisément, selon les considérants conclusifs de la décision :

> « (266) La Commission estime que le RGPD britannique et la DPA 2018 garantissent un niveau de protection des données personnelles transférées depuis l'Union européenne qui est substantiellement équivalent à celui garanti par le règlement (UE) 2016/679.
>
> (267) En outre, la Commission estime que, dans l'ensemble, les mécanismes de supervision et les voies de recours en vigueur au Royaume-Uni sont suffisants pour identifier et sanctionner en pratique les violations de la loi et offrent des voies de recours à la personne concernée pour obtenir l'accès aux données à caractère personnel la concernant et, éventuellement, la rectification ou l'effacement de ces données.
>
> (268) Enfin, sur la base des informations disponibles concernant l'ordre juridique britannique, la Commission considère que toute ingérence aux droits fondamentaux de la personne dont les données à caractère personnel sont transférées de l'Union européenne vers le Royaume-Uni par les autorités publiques britanniques à des fins d'intérêt public, notamment à des fins de répression et de sécurité nationale, sera limitée à ce qui est strictement nécessaire à la réalisation de l'objectif légitime en question et considère qu'il existe une protection juridique efficace contre de telles ingérences ».

Pour parvenir à cette conclusion, la Commission européenne a opéré une minutieuse analyse développée dans 88 pages portant sur plusieurs questions :

- le cadre juridique britannique de protection des données (en termes de protection constitutionnelle et législative, de champ d'application, de définitions, de garanties, de droits et d'obligations, de supervision et de concrétisation) dont la similitude avec le RGPD ressort du projet de décision comme étant évidente.

Les considérants 75 à 82 du projet de décision décrivent les dispositions du Royaume-Uni relatives à des transferts ultérieurs. Cependant, la Commission étant consciente que le pays pourrait devenir une porte dérobée pour des transferts de données personnelles de l'UE vers les États-Unis, il est quelque peu surprenant que le projet de décision ne mentionne ni l'arrêt *Schrems II*, ni la révision en cours des clauses contractuelles types, ni les recommandations du CEPD sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données personnelles de l'UE adoptés en novembre 2020[20].

- le cadre juridique d'accès et d'utilisation par des autorités publiques britanniques des données transférées par l'UE (cadre légal général, et spécifique aux finalités de sécurité nationale).

Dans les considérants 112 à 265, la Commission expose minutieusement les bases juridiques, les limites et les garanties des divers instruments que les services répressifs et les services de renseignement britanniques ont à leur disposition, la structure de contrôle en place, ainsi que le mécanisme de recours à la disposition des autorités compétentes et les personnes concernées.

Finalement, la Commission précise que toute ingérence dans ce domaine doit être limitée au strict nécessaire en constatant que des voies de recours existent au Royaume-Uni. On peut néanmoins se demander si par une telle formulation la Commission ne se trompe pas de rôle dans la mesure où celui-ci consiste en principe à constater et évaluer le niveau adéquat du droit britannique tel qu'il existe aujourd'hui et non à présumer que le Royaume-Uni encadrera bien les ingérences qu'il considèrera nécessaires.

La Commission souligne par ailleurs que sa conclusion se fonde non seulement sur un examen des lois nationales en vigueur au Royaume-Uni mais également sur l'adhésion de ce pays à la Convention européenne des droits de l'Homme et donc sa soumission à la juridiction de la Cour européenne des droits de l'Homme (CrEDH).

À l'issue de son analyse, tout le droit britannique lui paraît « essentiellement équivalent » à celui de l'UE, un constat qui lui permet de proposer l'adoption d'une décision d'adéquation en présumant ce faisant que le Brexit n'aura aucune incidence négative sur la protection des données personnelles et serait donc à ce sujet négligeable.

En outre, précisons que cette décision serait juridiquement contraignante au même titre que le RPGD. Elle engagera ainsi tous les États membres de l'UE qui devront donc se conformer à cette présomption de niveau équivalent et autoriser les transferts de données sans requérir aucun autre type d'autorisation.

[20] EDBB, *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*, Adoptées le 10 novembre 2020, 43 p.

La Commission rappelle cependant, en vertu de l'article 58(5) RGPD et de la jurisprudence *Schrems II*, que la mise en question d'une décision d'adéquation est possible devant la CJUE. En effet, elle précise :

> « Schrems II 120 Ainsi, même en présence d'une décision d'adéquation de la Commission, l'autorité nationale de contrôle compétente, saisie par une personne d'une réclamation relative à la protection de ses droits et de ses libertés à l'égard d'un traitement de données à caractère personnel la concernant, doit pouvoir examiner, en toute indépendance, si le transfert de ces données respecte les exigences posées par le RGPD et, le cas échéant, introduire un recours devant les juridictions nationales afin que ces dernières procèdent, si elles partagent les doutes de cette autorité quant à la validité de la décision d'adéquation, à un renvoi préjudiciel aux fins de l'examen de cette validité (voir par analogie, en ce qui concerne l'article 25, paragraphe 6, et l'article 28 de la directive 95/46, arrêt du 6 octobre 2015, Schrems, C-362/14, EU:C:2015:650, points 57 et 65) ».

Il convient en outre de souligner que cette décision serait inédite parce qu'il s'agit d'une évaluation d'un ex-membre de l'UE, mais également au regard de sa longueur et surtout de la clause de temporisation qu'elle contient (« *sunset clause* »).

En effet, cet élément nous semble très important étant donné que pour la première fois pour une décision de ce type la Commission a posé une limite à la validité de son acte, fixée à quatre ans. Parfaitement consciente que « le danger » pour les données de l'UE ne réside pas dans les lois britanniques actuelles sur la protection de la vie privée mais dans ce à quoi ces lois pourraient ressembler à l'avenir, elle a introduit cette clause dans les paragraphes 281-282 de son projet de décision avec la possibilité d'une prorogation de quatre ans.

Au regard de ces considérations, nous pourrions conclure, à l'instar de la Commission européenne dans ce projet, que l'impact du Brexit serait minime pour la protection des données personnelles étant donné que la législation britannique est très proche de la réglementation européenne, mais aussi parce que les mesures légales nécessaires ont été adoptées pour s'assurer que les droits des citoyens européens ne seront pas transgressés.

II. Un impact de fait important

Cette situation rassurante n'est néanmoins qu'une façade. Les garde-fous démocratiques que prévoit l'ordre juridique européen permettent de mettre en question le projet de décision relatif à l'adéquation du Royaume-Uni qui nous permet contestable. En effet, la procédure d'adoption de la décision d'adéquation exige de la Commission européenne de demander l'avis, non contraignant certes mais non moins influent, du CEPD selon l'article 70 (1-s) RGPD. En outre, le Parlement européen peut, à tout moment, demander à la Commission de maintenir, modifier ou retirer une décision d'adéquation.

Ces deux acteurs ont déjà réagi en fustigeant le projet de décision de la Commission européenne qui doit ainsi soit l'amender, soit l'adopter au risque de se trouver sanctionnée par la CJUE qui s'est montrée dernièrement très exigeante en matière de transferts de données (v. surtout *Schrems II*).

Cette situation est inquiétante pour plusieurs raisons.

Tout d'abord, il existe un risque en termes de sécurité juridique à l'égard du cadre légal britannique inconnu après le 30 juin 2021. Ensuite, elle dissimule des contradictions profondes entre la protection britannique et la protection européenne des données personnelles. Enfin, elle est révélatrice de paradoxes internes au système européen de protection des données.

1. Du point de vue britannique

Les défis que devait relever la Commission européenne sont de plusieurs ordres :

a. Une modification annoncée des règles de protection des données du droit britannique ;
b. L'exception en matière de données traitées pour des fins de contrôle de l'immigration ;
c. Les transferts ultérieurs de données personnelles ;
d. Loi et pratiques de surveillance : l'accès des autorités publiques aux données transférées au Royaume-Uni ;
e. Les faiblesses de la mise en application du droit de protection des données personnelles.

a. Une modification annoncée des règles de protection des données du droit britannique

Le premier défi, d'ordre général, concerne le suivi de l'évolution du système juridique britannique en matière de protection des données au regard d'une volonté politique ambitieuse de profonde modification. En effet, le gouvernement britannique a fait part de son intention d'élaborer des politiques distinctes et indépendantes en matière de protection des données caractérisée par une apparente volonté de s'écarter de la législation européenne en la matière tout en souhaitant obtenir une décision d'adéquation de la part de la Commission européenne.

En effet, le Premier ministre Boris Johnson a décla é : « *The UK will in future develop separate and independent policies in areas such as (but not limited to) … data protection, maintaining high standards as we do so* »[21].

Son conseiller principal entre 2019-2020, Dominic Cummings, est allé encore plus loin en affirmant :

> « *One of the many advantages of Brexit is we will soon be able to bin such idiotic laws* » ; « *We will be able to navigate between America's poor protection of privacy and the EU's hostility to technology and entrepreneurs* »[22].

Il existe donc une ambition de mettre en place une stratégie nationale favorable à la croissance, révélant la volonté du Royaume-Uni de construire une économie des données de premier plan au niveau mondial tout en souhaitant garantir la confiance du public dans l'utilisation de ces données. Cette stratégie, dénommée *National Data Strategy* ou NDS[23], a été rendue publique dans un rapport le 9 décembre 2020. Alors que ce document démontre clairement que Royaume-Uni veut prendre ses distances avec l'UE en matière de protection des données, il est

[21] House of Commons, Prime Minister, UK/EU relations, Statement made on 3 February 2020

[22] Daniel BOFFEY, "Dominic Cummings' data law shake-up a danger to trade, says EU", *The Guardian*, 25 September 2020

[23] Department for Digital, Culture, Media & Sport, *UK National Data Strategy*, Undated 9 December 2020

en même temps affirmé que le fait d'obtenir une décision d'adéquation au RGPD et à la Directive Police Justice fait partie de ses objectifs gouvernementaux[24].

Ces déclarations politiques ne se sont pas encore concrétisées, cependant cette éventuelle future divergence pourrait engendrer des risques en termes de maintien du niveau de protection des données personnelles transférées depuis l'UE.

C'est pour cette raison qu'aussi bien le Parlement européen que le CEPD ont mis la Commission européenne en garde devant le danger de reconnaître l'adéquation de la législation britannique, et donc de libérer les transferts de données, à un pays qui s'est déjà engagé dans un projet de profonde modification de son cadre national ayant pour fil conducteur de « déverrouiller le pouvoir des données pour le Royaume-Uni »[25].

La Commission européenne a néanmoins trouvé une solution originale pour prévenir ce risque en prévoyant, on l'a déjà mentionné, une « clause de temporisation » (« *sunset clause* ») ; une disposition qui apparaît pour la première fois dans un projet de décision d'adéquation. Ce faisant, on l' a déjà noté, la Commission a attribué une durée de validité de quatre ans à la décision d'adéquation, renouvelable une fois.

b. L'exception en matière de données traitées pour des fins de contrôle de l'immigration

Prévue à l'annexe 2, partie 1, paragraphe 4, l' « exception immigration » du *Data Protection Act* 2018, en vigueur depuis le 25 mai 2018, est l'un des éléments qui pourrait bloquer la prise d'une décision d'adéquation.

Aux termes de ce paragraphe, plusieurs droits prévus par le RPGD (droit à l'information, droit d'accès, droit de bénéficier de garanties en cas de transferts ultérieurs de données, droit de rectification, etc.) se trouvent écartés lorsque le traitement de données personnelles est justifié par une finalité d'efficacité du contrôle migratoire britannique.

> (« *the disclosure of that data would "prejudice" the maintenance of effective immigration control", or "the investigation or detection of activities that would undermine the maintenance of effective immigration control"* »).

Concrètement, cette exception offre une base légale à des organismes publics ou privés, responsables de traitements de données personnelles, pour opposer à un citoyen non-britannique l'« exception immigration » au motif que l'exercice de ses droits pourrait mettre en péril le maintien d'un contrôle effectif de l'immigration ou l'investigation et la détection d'activités nuisibles à l'effectivité du contrôle.

Ce n'est pas tant la finalité de cette exception qui pose question mais la rédaction trop large et générale avec laquelle elle a été formulée. L'expression « contrôle de l'immigration » désigne-t-elle un contrôle d'actes pénalement répréhensibles, comme le dépassement de la durée de validité d'un visa, ou bien inclue-t-elle aussi toute vérification de routine du statut d'un citoyen non-britannique ?[26]

---

[24] *Ibidem*. "*We will seek positive adequacy decisions from the EU, under both the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED), before the end of the transition period*".

[25] "*This strategy sets out how best to unlock the power of data for the UK*".

[26] "the term "immigration control" isn't defined. Does it mean any criminal act such as overstaying a visa? Maybe. Does it mean routine checking up of a person's immigration status? Perhaps. Will the exemption be applied against the routine or the exceptional? Unclear, and political promises mean nothing when the letter of law is this vague". Source : https://www.openrightsgroup.org/blog/what-is-at-stake-with-the-immigration-exemption-legal-challenge/

Cette situation a conduit deux ONG (l'une de défense de la vie privée et de la liberté d'expression en ligne -Open Rights Group- et l'autre de défense des citoyens européens qui veulent continuer à vivre au Royaume-Uni – 3million-) résidant au Royaume-Uni de demander à la High Court britannique d'apprécier la légalité de cette exception et sa conformité aux articles 7, 8 et 21 de la Charte des droits fondamentaux de l'UE (relatifs respectivement à la vie privée, aux données personnelles et à la non-discrimination).

Dans son arrêt *Open Rights Group & Anor, R (On the Application Of) v. Secretary of State for the Home Department & Anor*[27] du 3 octobre 2019, la High Court a cependant considéré que la disposition en question a un champ d'application suffisamment étroit et clair, poursuit un but légitime et est justifiée par un intérêt public important.

Alors que les requérants ont fait appel et que l'arrêt final n'avait pas encore été adopté[28], la Commission européenne a par ailleurs considéré que :

> « Bien que formulée de manière assez large, la restriction en matière d'immigration telle qu'interprétée par la jurisprudence et les orientations données par l'ICO est soumise à un certain nombre de conditions strictes - très similaires à celles fixées par le droit européen pour les restrictions aux droits et obligations en matière de protection des données - qui encadrent son application. En particulier, elle doit être appliquée au cas par cas, uniquement dans la mesure nécessaire pour atteindre un objectif légitime et de manière proportionnée »[29].

Néanmoins, notons qu'un document de l'ONG Open Rights Group, publié à la suite du projet de décision d'adéquation de la Commission, a mis en évidence la fréquence avec laquelle cette exception a été utilisée entre janvier 2020 et décembre 2020 (72,6%) et le fait que le ministère de l'Intérieur britannique n'a pas communiqué combien de recours ont été effectués contre l'application de l'exception[30].

Le CEPD a alors exigé que la décision finale de la Commission soit prise en tenant compte d'informations supplémentaires sur l'exemption d'immigration, en particulier en ce qui concerne la nécessité et la proportionnalité d'une exemption aussi largement admise.

Ce qui est certain est qu'après le 1er juillet 2021, le Royaume-Uni sera entièrement libre de poursuivre sa politique migratoire sans qu'il soit lié ni par le RGPD ni par la jurisprudence de la CJUE, à moins que les négociations avec la Commission puissent faire évoluer la politique migratoire du Royaume-Uni. Cette perspective nous paraît toutefois peu probable, surtout en ce qui concerne une question aussi sensible en termes d'expression de la souveraineté.

c. Les transferts ultérieurs de données personnelles

Un autre élément qui peut potentiellement justifier une décision d'inadéquation de la législation du Royaume-Uni aux standards européens est l'impossibilité de l'ordre juridique britannique d'assurer un niveau de protection suffisant des données personnelles lors de transferts ultérieurs avec des pays tiers (autres que l'UE).

---

[27] High Court, *Open Rights Group & Anor, R (On the Application Of) v. Secretary of State for the Home Department & Anor* [2019] EWHC 2562 (Admin), paragraphes 40 et 41.

[28] Elle a été adoptée le 11 octobre 2011, Court of Appeal (Civil Division), *Open Rights Group v Secretary of State for the Home Department and Secretary of State for Digital, Culture, Media and Sport*, [2021] EWCA Civ 800, points 53 à 56 : infirme la decision de la High Court

[29] Considérant 65 du projet de décision d'adéquation au RGPD.

[30] Source : https://www.openrightsgroup.org/publications/submission-to-the-european-commission-and-the-european-data-protection-board-on-the-operation-of-the-uks-immigration-exemption-in-the-data-protection-act-2018/

En effet, l'article 44 du GDPR prévoit que les transferts et les transferts ultérieurs de données à caractère personnel ne peuvent avoir lieu que si le niveau de la protection des personnes physiques garantie par le GDPR n'est pas réduit. Cela signifie que non seulement la législation britannique doit être « essentiellement équivalente » à la législation de l'UE en ce qui concerne le traitement des données à caractère personnel transférées au Royaume-Uni en vertu de la décision d'adéquation, mais aussi que les règles applicables au Royaume-Uni en ce qui concerne le transfert ultérieur de ces données vers des pays tiers doivent garantir qu'un niveau de protection essentiellement équivalent continuera d'être assuré.

Or, il convient de remarquer que le Royaume-Uni, depuis qu'il est devenu un État tiers à l'UE, détient le pouvoir souverain de déterminer ses propres conditions d'adéquation de son ordre juridique avec ceux d'autres États tiers. En ce sens, le pays pourrait déclarer que des territoires étrangers disposent d'un niveau de protection « essentiellement équivalent » au sien mais qui pourrait ne pas correspondre au niveau « essentiellement équivalent » de l'UE. Une telle situation impliquerait des risques pour les données des citoyens européens qui seraient transférées sur la base d'une décision d'adéquation britannique moins exigeante que l'adéquation européenne.

De plus, pour les territoires que le Royaume-Uni ne déclarera pas équivalents à son système juridique, seront utilisés des instruments de transferts contractuels prévus par le législateur britannique et potentiellement plus souple que les instruments européens de transferts vers des pays tiers.

Mais avant de s'inquiéter des décisions futures de transferts de données personnelles du Royaume-Uni, il convient de remarquer, à l'instar du Parlement européen, qu'à l'heure actuelle ce pays a déjà conclu des accords d'échanges de données avec des services du renseignement étrangers dont la seule existence pourrait justifier un refus de considérer le niveau « essentiellement équivalent » de sa législation à celle de l'UE. Ainsi, la *Five Eyes Intelligence Alliance* regroupe les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle Zélande. Or, l'arrêt *Schrems II* de la CJUE ayant jugé que le niveau de protection des États-Unis ne satisfait pas aux exigences européennes, cet accord auquel prend part le Royaume-Uni, pourrait théoriquement conduire au refus de la reconnaissance d'une adéquation.

En outre, les droits des citoyens européens se trouvent déjà transgressés par l'existence du *UK-US Cloud Agreement*, malgré les différentes garanties prévues. En effet, en vertu de cet accord, le Royaume-Uni peut être conduit à divulguer des données personnelles localisées sur son territoire ; une possibilité à propos de laquelle le Parlement européen alarme la Commission européenne depuis 2019.

d. Loi et pratiques de surveillance : l'accès des autorités publiques aux données transférées au Royaume-Uni

D'après une intéressante étude de terrain[31] de la doctrine spécialisée en matière de protection des données personnelles au Royaume-Uni, le point le plus épineux, qui devrait à lui tout seul écarter une décision d'adéquation de notre point de vue, est celui des pratiques de surveillance effectuées par le Royaume-Uni.

[31] D. KORFF and I. BROWN, *The inadequacy of UK data protection law*: Executive Summary / Part 1: General inadequacy / Part 2: UK surveillance, Data protection and digital competition blog, 9 October- 30 November 2020.

En particulier, des universitaires soutiennent que le gouvernement britannique [*Communications Headquarters* (GCHQ)] intercepte, conserve et analyse des masses de données personnelles, entre autres, en collaborant avec des acteurs privés ou en les obligeant à fournir des points d'accès à des câbles de communication sous-marins. Ces données sont utilisées pour enquêter sur les communications d'individus déjà connus « comme représentant une menace » ou pour générer de nouvelles pistes de renseignement, c'est-à-dire concernant des « personnes d'intérêt » jusqu'alors inconnues. Les experts soupçonnent fortement que de telles technologies d'extraction de données massives et leur traitement automatisé, notamment les traitements basés sur l'intelligence artificielle, soient largement déployés, par exemple pour identifier des individus en tant que terroristes.

Or, de telles pratiques posent des questions non seulement propres aux traitements algorithmiques, à savoir « l'erreur de taux de base » - le fait mathématiquement inévitable d'un grand nombre de faux positifs ou de faux négatifs lors de la recherche de cas rares dans de grands ensembles de données – mais également au regard de l'opacité de ce type de traitement - « phénomène de boîte noire » -.

Surtout, ces activités sont en contradiction avec le cadre européen de protection des données issu aussi bien de la jurisprudence de la CrEDH (par exemple, les arrêts *Klaas*, *Malone*, *Zakharov*, *Big Brother Watch and others*)[32] que de celle de la CJUE (par exemple, les arrêts *Schrems I*, *Schrems II*, *La Quadrature du Net*), mais également avec les recommandations du CEPD sur « les garanties européennes essentielles en matière de surveillance » du 10 novembre 2020.

En outre, le *UK Investigatory Powers Act* de 2016, qui fait partie du cadre légal britannique de protection des données personnelles, prévoit certes un grand nombre de garanties qui ont été mises en lumière par la Commission européenne en vue de fonder sa décision d'adéquation mais il contient également des règles permettant une extraction sans discrimination de l'ensemble des métadonnées de toutes les communications qui transitent sur la sol britannique.

Cette possibilité est en contradiction avec la jurisprudence de la CJUE de décembre 2020 *La Quadrature du Net*[33] selon laquelle « une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire et limitée aux données de localisation des personnes à l'égard desquelles, il existe une raison valable de soupçonner qu'elles sont impliquées d'une manière ou d'une autre dans des activités de terrorisme ».

La Commission européenne consacre de longs développements afin de soutenir sa position sur le niveau « essentiellement équivalent » du Royaume-Uni mais il paraît peu probable qu'elle ne se rende pas compte de la difficulté d'admettre une telle affirmation devant de tels faits.

Or, à moins que le législateur européen n'envisage d'aligner sa législation sur celle du Royaume-Uni en matière de collecte massive de données, en contradiction avec la jurisprudence récente de la CJUE, on ne peut qu'adhérer massivement à l'humour noir du rapport de Douwe Korff intitulé « *The inadaquacy of the EU Commission Draft GDPR Adequacy Decision on the UK* » dans lequel est ironiquement comparée l'évaluation de la Commission à propos des pratiques de surveillance britanniques aux trois signes de la sagesse : « Ne pas voir le Mal, ne pas entendre le Mal, ne pas dire le Mal ».

---

[32] CEDH, *Klaas*, 6 septembre 1978 ; *Malone*, 2 août 1984 ; *Weber and Saravia*, 29 juin 2006 ; *Liberty*, 1 juillet 2008; *Kennedy*, 18 mai 2010 ; *Zakharov*, 4 décembre 2015 ; *Big Brother Watch and others*, 4 février 2019.

[33] CJUE, 6 octobre 2020, *La Quadrature du Net et autres*, aff. jointes C-511/18, C-512/18 and C-520/18.

e. Les faiblesses de la mise en application du droit de protection des données personnelles

Alors que la Commission, dans les considérants 92 à 98 de son projet de décision d'adéquation, se félicite des pouvoirs de l'Autorité britannique de protection des données (ICO) et de la mise en application effective de la protection des données personnelles, Douwe Korff, spécialiste de la question, a fustigé la « politique de l'autruche » et la superficialité du raisonnement de l'institution européenne qui expose des affirmations contradictoires.

Il démontre ainsi, par un simple raisonnement mathématique, qu'« alors que l'ICO [selon ses propres dires issus de son rapport annuel 2019-2020] a examiné environ 28 000 cas, et qu'il y a eu environ 10 000 cas dans lesquels l'ICO a constaté que la loi avait été violée, les plaintes n'ont été officiellement "confirmées" que dans environ 730 cas (<3%), et il n'y a eu une mise en application "dure" [donc une sanction] que dans 24 cas (sous la forme de 22 avis de pénalité et de 2 avis d'exécution émis), c'est-à-dire dans moins de 0,025 % des cas »[34].

Nous partageons entièrement la conclusion de Douwe Korff selon laquelle, « il est difficile de voir comment la Commission - si elle avait examiné les statistiques ci-dessus - aurait pu conclu que l'ICO "identifie et punit" les transgresseurs "dans la pratique" et "impose des sanctions [appropriées]" aux responsables du traitement et aux sous-traitants qui enfreignent la loi ».

Ce raisonnement est d'autant plus pertinent que selon les critères européens de référence pour reconnaître l'adéquation [35], « la personne devrait être en mesure d'exercer des voies de recours pour faire valoir ses droits rapidement et effectivement, sans coût prohibitif, et pour assurer le respect des règles. Pour ce faire, il convient de mettre en place des mécanismes de contrôle permettant d'enquêter sur les plaintes de manière indépendante et de détecter et de sanctionner en pratique toute infraction du droit à la protection des données et au respect de la vie privée. Si les règles ne sont pas respectées, la personne concernée devrait également disposer de recours judiciaires et administratifs effectifs, y compris pour la réparation du préjudice subi en raison du traitement illicite des données à caractère personnel la concernant. Il s'agit d'un élément essentiel qui nécessite un système d'arbitrage indépendant permettant de réparer le dommage et d'imposer des sanctions le cas échéant ».

2. Du point de vue du droit européen

Notre recherche relative à l'impact du Brexit sur la protection des données personnelles a par ailleurs mis en lumière des paradoxes internes au système européen de protection des données qui peuvent se résumer de la manière suivante : d'une part, le caractère improbable de la reconnaissance d'une inadéquation du droit britannique qui laisserait apparaître des failles internes au système de l'UE ; le caractère contestable de la reconnaissance d'une adéquation qui braderait la protection des données au nom de la nécessité de libres transferts de données avec le Royaume Uni.

i. L'improbable inadéquation

[34] D. KORFF, "The inadequacy of the EU Commission Draft GDPR Adequacy Decision on the UK", *Data protection and digital competition blog*, 3 mars 2021, pp. 22-24.

[35] WP254rev01, section C.4.

Il est intéressant de relever la difficulté d'admettre que l'ordre juridique britannique n'est ni « équivalent », ni -encore moins- « substantiellement équivalent » à la protection européenne comme l'exige désormais la CJUE, qui repose sur deux principaux arguments.

Tout d'abord, comment peut-on admettre qu'un ordre juridique qui a été jusqu'à récemment un État membre de l'UE de longue date ne dispose pas d'un cadre juridique substantiellement équivalent à celui des autres États membres puisqu'il était censé avoir transposé la directive 95/46/CE et avoir incorporé le RGPD dans son ordre juridique -ce qu'il a d'ailleurs fait- ? Admettre aujourd'hui une inadéquation voudrait dire qu'un recours en manquement aurait dû être engagé par la Commission européenne (comme elle a su le faire contre l'Allemagne, la Hongrie, l'Autriche) à l'encontre du Royaume-Uni (sachant que sous le régime de la directive 95/46/CE, le pays n'avait pas correctement transposé ce texte). De plus, aucun communiqué de presse de la Commission depuis l'entrée en vigueur du RGPD n'a été publié. Ainsi, l'institution européenne n'a jamais fait usage de ses pouvoir pour mettre en demeure le Parlement britannique en vue de modifier son cadre juridique au regard de toutes les failles qu'il comporte.

Il était donc compliqué, en 2021, de déclarer cet ordre juridique inadéquat et non équivalent à la protection européenne.

Ensuite, l'inadéquation est une solution qui ne peut pas facilement être décidée car l'Union européenne est consciente des limites substantielles que présentent les instruments alternatifs à la décision d'adéquation, à savoir les CCT, les BCR, les codes de conduite, la certification ou labélisation ainsi que d'autres procédés prévus par l'article 42 du RGPD (consentement explicite, nécessité pour exécuter un contrat, etc.).

Les limites substantielles de ces instruments sont intéressantes sur un plan théorique mais elles nous intéressent plus pratiquement ici dans la mesure où il est probable de les voir s'appliquer un jour dans le cas de transferts entre l'UE et le Royaume-Uni.

Plusieurs limites à ces instruments peuvent en effet être relevées. En premier lieu, depuis l'arrêt *Schrems II,* la CJUE exige que l'exportateur et l'importateur de données évaluent en pratique si la législation du pays tiers permet de respecter le niveau de protection requis par le droit de l'UE et les garanties fournies par ces instruments.

Ainsi, l'on se trouve dans cette situation paradoxale, et à notre sens scandaleuse du point de vue de la protection des droits de personnes, qui ferait reposer sur les acteurs contractants, qui ont tout intérêt à échanger des données, la responsabilité de l'appréciation du niveau d'adéquation de la législation d'un État tiers. Par ailleurs, d'après ce même arrêt, si ce niveau européen ne peut être respecté par un État tiers, les entreprises doivent prévoir des mesures supplémentaires en vue de garantir un niveau de protection essentiellement équivalent à celui prévu dans l'Espace économique européen et doivent s'assurer que la législation de ce pays n'empiétera pas sur ces mesures supplémentaires de manière à les priver d'effectivité.

Or, on peut légitimement se demander comment les entreprises peuvent-elles savoir quelles sont ces mesures supplémentaires ? En outre, comment garantir que ces mesures seront respectueuses des droits qui découlent du RGPD ? Les organes de l'UE tentent actuellement de répondre à cette question qui fragilise temporairement tous les instruments alternatifs de transferts.

Surtout, il est étonnant que la nécessité de transférer des données personnelles neutralise toute possibilité d'interdire tout simplement le transfert vers un pays « dangereux » en termes européens.

En outre, la Commission européenne était en train de procéder (au moment des deux projets d'adéquation en question) à une modification des CCT[36], une démarche qui neutralisait la possibilité de reconnaître une inadéquation sachant que cet instrument est le choix n° 1 des entreprises lorsqu'elles transfèrent des données en dehors de l'UE.

Enfin les CCT et les BCR sont des instruments qui n'engagent que les parties contractantes et ne peuvent donc être opposés, par exemple, à des autorités publiques qui souhaiteraient accéder à des données.

Par conséquent, au regard de la nécessité d'occulter le fait qu'au sein même de l'UE il existe des États qui incorporent le droit européen de façon contraire à ses normes fondamentales *et* des limites des instruments alternatifs aux transferts à l'heure actuelle, on comprend bien que refuser de reconnaître le niveau « substantiellement équivalent » de la législation du Royaume-Uni à la législation européenne est presque une décision qui s'impose à la Commission.

ii. La contestable adéquation

Alors que la décision d'adéquation paraît s'imposer au regard des considérations précédemment exposées, comment ne pas voir que celle-ci ne peut être décidée sans que la protection des données personnelles ne soit mise à mal. Tout d'abord, on peut considérer qu'une décision d'adéquation transgresserait le standard européen des données personnelles que la CJUE essaie de construire. En effet, comment d'une part avoir invalidé le *Privacy Schield*, et donc affirmer que les États-Unis constituent un ordre juridique dangereux en termes de protection de données, et d'autre part admettre que l'adéquation du droit du Royaume-Uni qui a signé des accords d'échange de données avec ce pays.

On peut également envisager que le projet de décision vise à imposer un nouveau standard européen satisfaisant le *Brussels effet* en cherchant à lier les mains du législateur britannique s'agissant de futures modifications de son cadre juridique national ; le tout au détriment des droits des personnes dont les données continueront à transiter vers un pays qui ne correspond pas au modèle européen de protection des données à caractère personnel.

In fine, il s'agissait pour la Commission de choisir entre Charybde et Scylla, à savoir laquelle des deux options qui lui sont présentées - décision d'inadéquation ou décision d'adéquation - lui permettrait de ne pas trop trahir le modèle européen sans néanmoins trop le défendre non plus.

[36] La décision d'exécution relative aux nouvelles CCT a été adoptée le 4 juin 2021 : Commission européenne, *décision d'exécution (UE) 2021/319 de la Commission relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu du règlement (UE) 2016/679 du Parlement européen et du Conseil*, 4 juin 2021, JOUE, L 199/31 du 07.06.2021