
# Avis 14/2021 concernant le projet de décision d'exécution de la Commission européenne conformément au règlement (UE) 2016/679 constatant le niveau de protection adéquat des données à caractère personnel assuré par le Royaume-Uni

**Adopté le 13 avril 2021**

# TABLE DES MATIERES

**Le comité européen de la protection des données**

vu l'article 70, paragraphe 1, point s), du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après le «RGPD»),

vu l'accord sur l'Espace économique européen (ci-après l'«EEE») et, en particulier, son annexe XI et son protocole 37, tels que modifiés par la décision du Comité mixte de l'EEE nº 154/2018 du 6 juillet 2018[1],

vu les articles 12 et 22 de son règlement intérieur,

**A ADOPTÉ L'AVIS SUIVANT:**

# 1. RÉSUMÉ

1. La Commission européenne a approuvé son projet de décision d'exécution (ci-après le «projet de décision») constatant le niveau de protection adéquat des données à caractère personnel au Royaume-Uni en vertu du RGPD le 19 février 2021[2]. La Commission européenne a ensuite lancé la procédure en vue de son adoption formelle.

2. Le même jour, la Commission européenne a demandé l'avis du comité européen de la protection des données (ci-après l'«EDPB»)[3]. L'évaluation par l'EDPB concernant le caractère adéquat du niveau de protection des données à caractère personnel au Royaume-Uni a été effectuée sur la base de l'examen du projet de décision lui-même ainsi que d'une analyse de la documentation mise à disposition par la Commission européenne.

3. L'EDPB s'est concentré à la fois sur l'évaluation des aspects généraux liés au RGPD du projet de décision et sur l'accès des autorités publiques à des fins répressives et de sécurité nationale, aux données à caractère personnel transférées depuis l'EEE, y compris des voies de droit ouvertes aux citoyens de l'EEE. L'EDPB a également examiné si les garanties prévues par le cadre juridique britannique étaient en place et effectives.

[1] Dans le présent avis, on entend par «États membres» les «États membres de l'EEE».
[2] Voir le communiqué de presse de la Commission européenne intitulé «Protection des données: la Commission européenne engage un processus concernant les flux de données à caractère personnel vers le Royaume-Uni», 19 février 2021, disponible à l'adresse suivante: https://ec.europa.eu/commission/presscorner/detail/fr/ip_21_661.
[3] Idem.

4. L'EDPB a principalement utilisé dans ce cadre ses critères de référence pour l'adéquation dans le cadre du RGPD[4] adoptés en février 2018 et les recommandations 02/2020 de l'EDPB sur les garanties essentielles européennes pour les mesures de surveillance[5].

[4] Voir groupe de travail «article 29», critères de référence pour l'adéquation, adoptés le 28 novembre 2017, version révisée et adoptée le 6 février 2018, WP 254 rev.01, (approuvés par l'EDPB, voir https://edpb.europa.eu/node/1491_fr); (ci-après les «*critères de référence pour l'adéquation dans le cadre du RGPD*»).

[5] Voir les recommandations 02/2020 de l'EDPB sur les garanties essentielles européennes pour les mesures de surveillance, adoptées le 10 novembre 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_fr.

## 1.1. Domaines de convergence

5. L'objectif principal de l'EDPB est de donner un avis à la Commission européenne sur le caractère adéquat du niveau de protection garanti aux personnes physiques au Royaume-Uni. Il importe de noter que l'EDPB ne s'attend à ce que le cadre juridique britannique reproduise la législation européenne en matière de protection des données.

6. Toutefois, l'EDPB rappelle que, pour que le niveau de protection soit considéré comme adéquat, l'article 45 du RGPD et la jurisprudence de la Cour de justice de l'Union européenne (ci-après la «CJUE») exigent que la législation du pays tiers soit alignée sur l'essence des principes fondamentaux inscrits dans le RGPD. Le cadre du Royaume-Uni en matière de protection des données est en grande partie fondé sur celui de l'Union [notamment le RGPD et la directive (UE) 2016/680 du Parlement européen et du Conseil, ci-après la «directive en matière de protection des données dans le domaine répressif»], une conséquence du fait que le Royaume-Uni a été un État membre de l'Union européenne jusqu'au 31 janvier 2020. Par ailleurs, la loi britannique de 2018 sur la protection des données, qui est entrée en vigueur le 23 mai 2018 et a abrogé la loi britannique de 1998 sur la protection des données, transpose la directive relative à la protection des données dans le domaine répressif et précise en outre l'application du RGPD dans le droit britannique. Elle octroie également des pouvoirs et impose des devoirs à l'autorité nationale de contrôle de la protection des données, l'*Information Commissioner's Office* du Royaume-Uni (bureau du commissaire à l'information, ci-après l'«ICO»). L'EDPB reconnaît dès lors que le Royaume-Uni a en majeure partie reproduit le RGPD dans son cadre en matière de protection des données.

7. **Lors de l'analyse du droit et de la pratique d'un pays tiers qui, jusqu'à il y a peu, était encore un État membre de l'Union européenne, l'EDPB a en toute logique constaté que de nombreux aspects étaient substantiellement équivalents.**

8. Concernant la protection des données, l'EDPB observe qu'il existe une forte convergence entre le cadre du RGPD et le cadre juridique britannique concernant certaines dispositions fondamentales telles que des concepts (par exemple, «données à caractère personnel»; «traitement des données à caractère personnel»; «responsable du traitement des données»), les fondements du traitement loyal et licite pour des finalités légitimes, la limitation des finalités, la qualité et la proportionnalité des données, la conservation, la sécurité et la confidentialité des données, la transparence, les catégories particulières de données, la vente directe et la prise de décision automatisée et le profilage.

## 1.2. Défis

9. Jusqu'à il y a peu, le Royaume-Uni était encore un État membre de l'Union européenne: par conséquent, lors de l'analyse du droit et de la pratique du pays, l'EDPB a constaté que de nombreux aspects étaient substantiellement équivalents. Dans le même temps, au vu de son rôle dans le processus d'adoption d'une décision d'adéquation, mais également des contraintes de temps, l'EDPB a décidé de se concentrer sur les aspects qui méritent, selon lui, une plus grande attention et un examen plus approfondi.

10. Certains éléments restent néanmoins problématiques et l'EDPB estime qu'il convient d'approfondir l'analyse des points suivants afin de garantir un niveau de protection substantiellement équivalent. La Commission européenne devrait en outre suivre de près l'évolution de ces éléments au Royaume-Uni.

### 1.2.1. Généralités

11. Le premier élément problématique, d'ordre général, a trait au suivi de l'évolution du système juridique britannique en matière de protection des données dans son ensemble. En effet, le gouvernement britannique a fait part de son intention d'élaborer des politiques distinctes et indépendantes en matière de protection des données, et d'une éventuelle volonté de s'écarter du droit de l'Union en la matière. De telles déclarations politiques n'ont pas encore pris corps dans le cadre juridique du Royaume-Uni. Cette possible **divergence future pourrait toutefois être source de risques pour le maintien du niveau de protection des données à caractère personnel transférées depuis l'Union. La Commission européenne est ainsi invitée à surveiller de près de telles évolutions à partir de l'entrée en vigueur de sa décision d'adéquation et à prendre les mesures nécessaires, y compris en modifiant et/ou en suspendant la décision le cas échéant.**

### 1.2.2. Aspects généraux de la protection des données

12. Premièrement, la **dérogation concernant l'immigration**, visée à l'**annexe 2, partie 1**, paragraphe 4, **de la loi de 2018 sur la protection des données** est **formulée de manière générale**. En particulier, elle s'applique également si les données à caractère personnel ne sont pas collectées à des fins de contrôle de l'immigration par un responsable du traitement, mais sont communiquées par celui-ci à un autre responsable du traitement qui, lui, traite ces données à caractère personnel à des fins de contrôle de l'immigration.

13. L'EDPB invite la Commission européenne à vérifier l'état d'avancement de l'affaire *Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin)* et, étant donné que l'arrêt n'est pas définitif (autorité de la chose jugée), à vérifier si celui-ci est confirmé ou infirmé par l'arrêt attaqué, en tenant compte de toute évolution à cet égard, à le préciser dans la décision. **L'EDPB invite également la Commission européenne à fournir de plus amples informations sur la dérogation concernant l'immigration dans la décision d'adéquation[6], en particulier concernant la nécessité et la proportionnalité d'une dérogation si large prévue par le droit britannique, notamment à propos du large champ d'application ratione personae.** Dans le même temps, l'EDPB invite la Commission européenne à continuer de chercher si le cadre juridique britannique contient des garanties supplémentaires ou si celles-ci pourraient être envisagées, par exemple grâce à des instruments juridiquement contraignants qui compléteraient la dérogation concernant l'immigration en améliorant sa prévisibilité pour les personnes concernées et les garanties protégeant ces dernières, ce qui permettrait également d'assurer une évaluation et un suivi rapide et amélioré des exigences de nécessité et de proportionnalité.

14. Deuxièmement, même s'il reconnaît que le Royaume-Uni a en grande partie repris le chapitre V du RGPD dans son cadre relatif à la protection des données, l'EDPB a recensé certains aspects du cadre juridique britannique **relatifs aux transferts ultérieurs** qui pourraient compromettre le niveau de protection des données à caractère personnel transférées depuis l'EEE.

[6] Ainsi que dans les conclusions de l'examen en cours du recours à la dérogation concernant l'immigration auquel il est fait référence à la page 5 du *Explanatory Framework for Adequacy Discussions* (Cadre explicatif destiné aux discussions relatives à l'adéquation), section E3: limitations prévues à l'annexe 2, 13 mars 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf.

15. L'article 44 du RGPD[7] dispose en effet que les transferts et les transferts ultérieurs de données à caractère personnel ne peuvent avoir lieu que si le niveau de protection des personnes physiques garanti par le RGPD est respecté. **Dès lors, la législation britannique est non seulement «substantiellement équivalente» à la législation de l'Union concernant le traitement des données à caractère personnel transférées vers le Royaume-Uni au titre de la future décision d'adéquation, mais les règles applicables au Royaume-Uni en matière de transfert ultérieur desdites données vers des pays tiers garantissent également le maintien d'un niveau de protection substantiellement équivalent.**

16. Bien qu'il prenne note de la capacité du Royaume-Uni, au titre de son cadre juridique, à reconnaître que certains territoires offrent un niveau de protection des données adapté au regard du cadre du Royaume-Uni relatif à la protection des données, l'EDPB souhaite souligner qu'il est possible que de tels territoires peuvent, à ce jour, ne pas bénéficier d'une décision d'adéquation de la Commission européenne et garantir un niveau de protection «substantiellement équivalent» à celui assuré dans l'EEE. Cela pourrait entraîner d'éventuels risques en ce qui concerne la protection assurée pour les données à caractère personnel transférées depuis l'EEE en particulier si, à l'avenir, le cadre du Royaume-Uni relatif à la protection des données s'écartait de l'acquis de l'Union. En outre, le Royaume-Uni a déjà reconnu comme adéquats les pays tiers qui bénéficient d'une décision d'adéquation de la Commission européenne au titre de la directive 95/46/CE[8], tandis que la Commission européenne examinera bientôt ces décisions, et que les conclusions de cet examen ne sont pas encore connues.

17. **En ce qui concerne les situations susmentionnées, la Commission européenne devrait remplir son rôle de surveillance et, dans l'éventualité où le niveau de protection substantiellement équivalent des données à caractère personnel transférées depuis l'EEE ne serait pas maintenu, envisager de modifier la décision d'adéquation pour introduire des garanties spécifiques concernant les données transférées depuis l'EEE et/ou de la suspendre.**

18. **En ce qui concerne les accords internationaux conclus entre le Royaume-Uni et des pays tiers**, la Commission européenne est invitée à examiner les interactions entre le cadre du Royaume-Uni relatif à la protection de données et les engagements internationaux du Royaume-Uni, au-delà de l'accord sur l'accès aux données électroniques aux fins de la lutte contre la grande criminalité conclu entre le Royaume-Uni et les États-Unis d'Amérique[9] (ci-après l'«accord CLOUD Act»), notamment pour garantir la continuité du niveau de protection lorsque des données à caractère personnel sont transférées depuis l'Union vers le Royaume-Uni sur la base de la décision d'adéquation visant le

[7] «*Un transfert, vers un pays tiers ou à une organisation internationale, de données à caractère personnel qui font ou sont destinées à faire l'objet d'un traitement après ce transfert ne peut avoir lieu que si, sous réserve des autres dispositions du présent règlement, les conditions définies dans le présent chapitre sont respectées par le responsable du traitement et le sous-traitant, y compris pour les transferts ultérieurs de données à caractère personnel au départ du pays tiers ou de l'organisation internationale vers un autre pays tiers ou à une autre organisation internationale. Toutes les dispositions du présent chapitre sont appliquées de manière à ce que le niveau de protection des personnes physiques garanti par le présent règlement ne soit pas compromis.*»

[8] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO L 281 du 23.11.1995, p. 31).

[9] Voir l'accord entre le gouvernement du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord et le gouvernement des États-Unis d'Amérique relatif à l'accès aux données électroniques aux fins de la lutte contre la grande criminalité, Washington, États-Unis, 3 octobre 2019, disponible à l'adresse suivante: https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019.

Royaume-Uni et ensuite transférées ultérieurement vers d'autres pays tiers. La Commission est également invitée à assurer un suivi continu et à prendre des mesures, le cas échéant, si la conclusion d'accords internationaux entre le Royaume-Uni et des pays tiers risquait de compromettre le niveau de protection des données à caractère personnel garanti dans l'Union.

19. La Commission européenne est en outre invitée à vérifier si l'accord CLOUD Act offre des garanties supplémentaires adaptées, en tenant compte du niveau de sensibilité des catégories de données concernées et des seules exigences relatives au transfert de preuves électroniques effectué directement par des fournisseurs de service plutôt que par des autorités entre elles, en évaluant également dans quelles conditions il est possible d'offrir des garanties grâce à la bonne application de l'adaptation de l'accord UE-USA sur la protection des données à caractère personnel[10].

20. L'EDPB observe en outre que des transferts ultérieurs peuvent également avoir lieu depuis le Royaume-Uni vers un autre pays tiers au moyen d'**outils de transfert en application de la législation britannique en vigueur en matière de protection des données[11].** En vertu de l'arrêt *Schrems II*[12], l'EDPB invite la Commission européenne, dans la décision d'adéquation, à donner l'assurance que les garanties nécessaires seront effectivement mises en œuvre, en prenant également en considération la législation du pays tiers récepteur.

21. En ce qui concerne l'**absence des protections visées à l'article 48 du RGPD** dans la législation britannique, l'EDPB invite la Commission européenne à fournir des garanties supplémentaires et des références spécifiques à la législation britannique qui garantissent que le niveau de protection assuré en vertu du cadre juridique britannique est substantiellement équivalent au niveau de protection assuré dans l'EEE.

22. S'agissant des **mécanismes en matière de procédure et d'application**, l'EDPB fait remarquer que l'existence d'une autorité de contrôle indépendante fonctionnant de manière efficace, l'existence d'un système assurant un niveau de conformité satisfaisant, et d'un système d'accès aux mécanismes de recours appropriés permettant aux citoyens de l'EEE d'exercer leurs droits et de disposer de voies de recours administratives et judiciaires sans être confrontés à des obstacles majeurs sont autant de caractéristiques essentielles d'un cadre de protection des données conforme au cadre européen en la matière.

23. L'EDPB reconnaît que le Royaume-Uni a dans l'ensemble reproduit les dispositions pertinentes du RGPD dans le RGPD britannique et dans la loi de 2018 sur la protection des données; toutefois, la Commission européenne est invitée à suivre en permanence toute évolution du cadre et de la pratique juridiques britanniques qui pourraient avoir des effets négatifs dans ces domaines.

### 1.2.3. Accès des autorités publiques aux données transférées au Royaume-Uni

24. L'EDPB note les modifications considérables apportées au cadre juridique britannique applicable aux services de sécurité et de renseignement, notamment en ce qui concerne l'interception et l'acquisition des données de communication. L'EDPB comprend que ces modifications constituent, entre autres, une réponse aux procédures engagées devant la CJUE et la Cour européenne des droits

[10] Voir l'accord entre les États-Unis d'Amérique et l'Union européenne sur la protection des informations à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, décembre 2016 (ci-après l'«accord UE-USA sur la protection des données à caractère personnel»), disponible à l'adresse suivante: https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=LEGISSUM%3A3104_8.
[11] Voir les articles 46 et 47 du RGPD britannique.
[12] Voir l'arrêt *Schrems II*.

de l'homme (ci-après la «CouEDH») et les arrêts que celles-ci ont récemment rendus dans ce contexte.

25. L'EDPB se félicite en particulier de la création de l'Investigatory Powers Tribunal (le tribunal du Royaume-Uni chargé des pouvoirs d'enquête, ci-après l'«IPT»). L'IPT est compétent pour connaître des affaires relatives à l'utilisation des pouvoirs d'enquête non seulement par les autorités répressives mais également par les services de renseignement. Il est ainsi entendu par l'EDPB que l'IPT fonctionne comme un véritable tribunal au sens de l'article 47 de la charte des droits fondamentaux de l'Union européenne (ci-après la «charte de l'Union»).

26. L'EDPB relève avec satisfaction l'introduction de «commissaires judiciaires» dans la loi de 2016 sur les pouvoirs d'enquête (Investigatory Powers Act 2016, ci-après l'«IPA de 2016»), une amélioration non négligeable. De ce que l'EDPB comprend, l'une des fonctions importantes de ces commissaires judiciaires est d'approuver ex ante les différentes mesures de surveillance dans chaque cas particulier, y compris l'interception ciblée et l'acquisition en masse de données de communication (procédure dite de «double lock», double autorisation).

27. Cependant, afin d'évaluer l'efficacité de ce niveau supplémentaire de contrôle, l'EDPB estime nécessaire de préciser plus avant les scénarios dans lesquels une interception légale est possible sans approbation du commissaire chargé des pouvoirs d'enquête (Investigatory Powers Commissionner, ci-après l'«IPC») ou des commissaires judiciaires, et invite la Commission européenne à poursuivre son évaluation et à démontrer que, même dans les cas où la procédure de «double lock» ne s'applique pas, le cadre juridique britannique fournit des garanties adéquates, y compris grâce à un contrôle ex post efficace et aux possibilités de recours dont disposent les personnes, garantissant ainsi un niveau de protection substantiellement équivalent à celui assuré dans l'Union.

28. En outre, l'EDPB invite la Commission européenne à approfondir l'évaluation des conditions dans lesquelles l'urgence peut être invoquée, et à apporter des précisions sur les moyens possibles permettant aux personnes concernées d'exercer leurs droits et sur les voies de recours dont elles disposent dans le contexte d'opérations d'exploitation de réseaux informatiques, notamment dans le cas d'une dérogation à la procédure de «double lock».

29. L'EDPB estime en outre que les interceptions en masse doivent être davantage précisées et faire l'objet d'une évaluation plus poussée, notamment en ce qui concerne le choix et l'application des sélecteurs, afin de savoir exactement dans quelle mesure l'accès aux données à caractère personnel respecte le seuil établi par la CJUE, et quelles sont les garanties en place pour protéger les droits fondamentaux des individus dont les données sont interceptées dans ce contexte, y compris concernant les durées de conservation des données. Une évaluation indépendante réalisée par les autorités britanniques de contrôle compétentes serait particulièrement utile. L'EDPB souligne également que la situation semble d'autant plus critique que les «communications liées à l'outre-mer», qui tombent dans le périmètre des pratiques d'interception en masse, semblent impliquer que des données pourraient être directement interceptées et collectées en masse par le Royaume-Uni dans l'Union, y compris des données en transit entre l'Union et le Royaume-Uni, ce qui relève du champ d'application du projet de décision. Étant donné l'importance de cet aspect, l'EDPB invite la Commission européenne à suivre de près les évolutions à cet égard.

30. Toujours en ce qui concerne l'interception en masse, l'EDPB attire l'attention sur l'évaluation cohérente de la CouEDH et de la CJUE et rappelle les inquiétudes exprimées à l'égard des données secondaires, qui devraient faire l'objet de garanties spécifiques en raison de leur sensibilité. Aussi, l'EDPB invite la Commission européenne à minutieusement déterminer si les garanties offertes par

le droit britannique pour ces catégories de données à caractère personnel garantissent un niveau de protection substantiellement équivalent à celui assuré dans l'EEE.

31. Dans ce contexte, l'EDPB est conscient que le rapport public de 2016 de commission du parlement britannique chargée du contrôle des services de renseignement (Intelligence and Security Committee of Parliament) portant sur l'utilisation des pouvoirs aux fins des opérations de masse visant le recueil de données et de renseignements[13] concerne les pratiques découlant de l'ancien cadre juridique, lequel a ensuite été remplacé par l'IPA de 2016. Il estime néanmoins qu'une évaluation et un contrôle supplémentaires indépendants de l'utilisation d'outils de traitement automatisé par les autorités britanniques de contrôle compétentes sont nécessaires, et invite la Commission européenne à évaluer plus en profondeur cette question ainsi que les garanties qui seraient et/ou pourraient être accordées aux personnes concernées de l'EEE dans ce contexte.

32. L'EDPB partage l'avis de l'IPC selon lequel une évaluation et un suivi supplémentaires sont nécessaires pour veiller à ce que les garanties appliquées en pratique par les autorités compétentes dans le domaine de la sécurité nationale et du renseignement afin de lutter contre le non-respect de la législation concernée soient maintenues et constamment améliorées. L'EDPB se félicite également du fait que l'IPC ait dès lors procédé à un examen de son approche en matière d'inspection de l'interception en masse, en 2019, «*qui incluait un examen minutieux des moyens techniquement complexes par lesquels l'interception en masse est effectivement mise en œuvre*», et qu'il se soit engagé à inclure «*un examen détaillé des sélecteurs et des critères de recherche auxquels la CouEDH fait référence ci-dessus*» dans les inspections de l'interception en masse à partir de 2020. Compte tenu de l'importance de cet aspect, l'EDPB s'inquiète de ce que l'IPC n'ait pas encore procédé à un examen détaillé des sélectionneurs et des critères de recherche, et appelle la Commission européenne à contrôler étroitement les développements à cet égard, d'autant que le format concret de ces contrôles reste à préciser.

33. L'EDPB souligne qu'en ce qui concerne la divulgation outre-mer, l'application de l'exception de la sécurité nationale prévue par le droit britannique pourrait mener à une absence de garanties assurant le respect des principes de limitation des finalités, de nécessité et de proportionnalité, ou prévoyant des droits individuels, un contrôle et des voies de recours suffisants dans le pays tiers de destination. L'EDPB recommande ainsi à la Commission européenne de poursuivre son examen des garanties globales prévues dans le droit britannique concernant la divulgation outre-mer, notamment au regard de l'application des exceptions de la sécurité nationale.

34. Enfin, l'EDPB se dit préoccupé par d'autres formes de partage et de divulgation d'informations fondées sur d'autres instruments, notamment sur les divers accords internationaux conclus entre le Royaume-Uni et d'autres pays tiers, en particulier lorsque le public n'a pas accès à ces instruments, comme le *UK-US Communication Intelligence Agreement* (accord entre le Royaume-Uni et les États-Unis relatif à la communication de renseignements). L'incidence d'un tel accord pourrait entraîner un contournement des garanties liées à l'accès aux données à caractère personnel et à leur utilisation à des fins de sécurité nationale. L'EDPB estime que la conclusion d'accords bilatéraux ou multilatéraux avec des pays tiers à des fins de coopération en matière de renseignement, qui offrent une base juridique pour l'interception et l'acquisition directes de données à caractère personnel ou

[13] Voir le *Report of the bulk powers review* (Rapport de l'examen de l'utilisation des pouvoirs aux fins des opérations de masse visant le recueil de données et de renseignements) publié par l'Independent Reviewer of Terrorism Legislation, août 2016, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf.

pour le transfert de données à caractère personnel vers ces pays, pourrait également avoir des conséquences significatives sur les conditions de l'utilisation ultérieure des informations collectées, dans la mesure où ces accords sont susceptibles d'avoir des répercussions sur le cadre juridique britannique de la protection des données objet de l'évaluation.

### 1.3. Conclusion

35. L'EDPB estime que l'évaluation de l'adéquation du Royaume-Uni est un cas unique étant donné que ce pays est un ancien État membre de l'Union européenne. Il s'agirait en outre de la première décision d'adéquation comprenant une «clause de limitation dans le temps» (sunset clause).

36. L'EDPB reconnaît ainsi l'existence de nombreux domaines de convergence entre les cadres de protection des données du Royaume-Uni et de l'Union. Dans le même temps, à l'issue d'une analyse rigoureuse du projet de décision de la Commission européenne et de la législation britannique en matière de protection des données, l'EDPB a toutefois relevé un certain nombre de points problématiques qui sont examinés en détail dans le présent avis. L'EDPB souhaite dans ce contexte insister sur le rôle crucial que joue la Commission européenne dans le suivi de l'ensemble des évolutions pertinentes au Royaume-Uni.

37. Au vu des éléments susmentionnés, l'EDPB recommande à la Commission européenne de se pencher sur les points problématiques évoqués dans le présent avis. L'EDPB invite également la Commission à suivre de près toutes les évolutions pertinentes au Royaume-Uni susceptibles d'avoir une incidence sur l'équivalence substantielle du niveau de protection des données à caractère personnel, et, s'il y a lieu, à prendre les mesures appropriées dans les plus brefs délais.

## 2. INTRODUCTION

### 2.1. Le cadre du Royaume-Uni relatif à la protection des données

38. Le cadre du Royaume-Uni relatif à la protection des données est en grande partie fondé sur le cadre régissant la protection des données de l'Union européenne (en particulier le RGPD et la directive relative à la protection des données dans le domaine répressif), ce qui s'explique par l'appartenance du Royaume-Uni à l'Union européenne jusqu'au 31 janvier 2020. Par ailleurs, la loi britannique de 2018 sur la protection des données, qui est entrée en vigueur le 23 mai 2018 et a abrogé la loi britannique de 1998 sur la protection des données, transpose la directive relative à la protection des données dans le domaine répressif et précise en outre l'application du RGPD dans le droit britannique. Elle octroie également des pouvoirs et impose des devoirs à l'autorité nationale de contrôle de la protection des données, l'ICO.

39. Comme indiqué au considérant 12 du projet de décision de la Commission européenne, le gouvernement britannique a mis en œuvre la loi de 2018 sur l'Union européenne (retrait) [European Union (Withdrawal) Act 2018] qui intègre la législation de l'Union européenne directement applicable dans le droit britannique. En vertu de cette loi, les ministres du Royaume-Uni sont habilités à arrêter des dispositions d'application, par voie d'instruments de législation secondaire, pour apporter les modifications nécessaires au droit de l'Union conservé à la suite du retrait du Royaume-Uni de l'Union, afin qu'il corresponde au contexte national.

40. Par conséquent, le cadre juridique pertinent applicable au Royaume-Uni après la fin de la période de transition[14] est le suivant:

- le règlement général sur la protection des données du Royaume-Uni (ci-après le «RGPD britannique»), tel qu'il a été incorporé dans le droit britannique en vertu de la loi de 2018 sur l'Union européenne (retrait) et modifié par le règlement de 2019 portant, entre autres, modification des dispositions relatives à la protection des données, à la protection de la vie privée et aux communications électroniques dans le cadre de la sortie de l'Union européenne [Data Protection, Privacy and Electronic Communications (Amendment Etc.) (EU Exit)) Regulations 2019, le «règlement DPPEC de 2019»];
- la loi de 2018 sur la protection des données (Data Protection Act, ci-après la «DPA de 2018»), telle que modifiée par les règlements de 2020 relatifs à la protection des données, à la vie privée et aux communications électroniques (amendements, etc.) (retrait de l'UE) [Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (DPPEC Regulations)]; et
- l'IPA de 2016.

(l'ensemble formant le «cadre du Royaume-Uni relatif à la protection des données»).

## 2.2. Portée de l'évaluation de l'EDPB

41. Le projet de décision de la Commission européenne résulte d'une évaluation du cadre du Royaume-Uni relatif à la protection des données suivie de discussions avec le gouvernement du Royaume-Uni. Conformément à l'article 70, paragraphe 1, point s), du RGPD, l'EDPB est tenu d'émettre un avis indépendant sur les constats de la Commission européenne, de déterminer, le cas échéant, les insuffisances du cadre d'adéquation, et de présenter des propositions pour y remédier.

42. Comme mentionné dans les critères de référence pour l'adéquation dans le cadre du RGPD: «*les informations fournies par la Commission européenne devraient être exhaustives et permettre au comité de procéder à sa propre évaluation concernant le niveau de protection des données dans le pays tiers*»[15].

43. Notons à cet égard que l'EDPB n'a reçu en temps et en heure qu'une partie des documents pertinents pour l'examen du cadre juridique britannique. L'EDPB a reçu la plupart de la législation britannique à laquelle il est fait référence dans le projet de décision par les liens indiqués dans le projet. La Commission européenne n'a pas été en mesure de fournir des explications et engagements écrits de la part du Royaume-Uni s'agissant des échanges entre les autorités britanniques et la Commission européenne en lien avec le présent exercice[16].

[14] La fin de la période de transition est fixée au 31 décembre 2020, date après laquelle le droit de l'Union ne s'appliquera plus au Royaume-Uni. La période de transition se termine le 30 juin 2021 au plus tard, et fait référence à la période supplémentaire pendant laquelle la transmission de données personnelles depuis l'EEE vers le Royaume-Uni n'est pas considérée comme un transfert.
[15] Voir WP 254 rev.01, p. 3.
[16] En ce qui concerne: l'article 48 du RGPD (note de bas de page 78 du projet de décision); le renforcement des garanties et des mesures de sécurité appliquées par les responsables du traitement lors du traitement dans un contexte de sécurité nationale (note de bas de page 64 du projet de décision); l'exigence selon laquelle le responsable du traitement doit se demander s'il est nécessaire de faire appel à la dérogation au cas par cas même lorsqu'un certificat de sécurité national a été délivré (considérant 126 et note de bas de page 172 du

44. Compte tenu des éléments susmentionnés et en raison du délai restreint (deux mois) imparti à l'EDPB pour adopter le présent avis, celui-ci a choisi de se concentrer sur certains points spécifiques du projet de décision, et de proposer l'analyse qu'il en aura faite et son avis sur ceux-ci.

45. Lors de l'analyse du droit et de la pratique d'un pays tiers qui, jusqu'à il y a peu, était encore un État membre de l'Union européenne, l'EDPB a en toute logique constaté que de nombreux aspects étaient substantiellement équivalents. Eu égard à son rôle dans le processus d'adoption d'une décision d'adéquation et du volume de droit et de pratique à analyser, l'EDPB a décidé de concentrer son attention sur les aspects qui, à ses yeux, demandaient plus particulièrement à être étudiés. En outre, conformément à la jurisprudence de la CJUE, une très grande partie de l'analyse porte sur le régime juridique relatif à l'accès à des fins de sécurité nationale aux données à caractère personnel transférées vers le Royaume-Uni et sur la pratique de l'appareil national de sécurité au Royaume-Uni. Toutefois, il convient de garder à l'esprit que la sécurité nationale est manifestement un domaine du droit et de la pratique dans lequel la législation des États membres n'est pas harmonisée à l'échelle de l'Union et, partant, peut varier.

46. L'EDPB a tenu compte du cadre européen applicable en matière de protection des données, y compris les articles 7, 8 et 47 de la charte de l'Union, qui portent respectivement sur le droit au respect de la vie privée et familiale, sur le droit à la protection des données à caractère personnel et sur le droit à un recours effectif et à accéder à un tribunal impartial, et l'article 8 de la convention européenne des droits de l'homme (ci-après la «CEDH»), qui protège le droit au respect de la vie privée et familiale. Outre les éléments susmentionnés, l'EDPB a pris en considération les exigences du RGPD ainsi que la jurisprudence pertinente.

47. Cet exercice a pour objectif de donner un avis à la Commission européenne sur l'évaluation du caractère adéquat du niveau de protection au Royaume-Uni. Ce concept de «niveau de protection adéquat», qui existait déjà au titre de la directive 95/46, a été développé par la CJUE. Il importe de rappeler la norme définie par la CJUE dans l'arrêt *Schrems I*, à savoir que, si le «niveau de protection» dans le pays tiers doit être «substantiellement équivalent» à celui garanti dans l'Union, «*les moyens auxquels ce pays tiers a recours, à cet égard, pour assurer un tel niveau de protection peuvent être différents de ceux mis en œuvre au sein de l'Union*»[17]. Par conséquent, l'objectif n'est pas de refléter point par point la législation européenne, mais d'établir les exigences essentielles et fondamentales de la législation objet de l'examen. L'adéquation peut être obtenue en combinant les droits des personnes concernées et les obligations de ceux qui traitent les données ou qui exercent un contrôle

projet de décision); le fait que les protections de l'accord UE-USA sur la protection des données à caractère personnel s'appliqueront à l'ensemble des informations personnelles produites ou protégées au titre de l'accord CLOUD Act, indépendamment de la nature ou du type d'organisme à l'origine de la demande, en ce qui concerne les éléments de la mise en œuvre concrète des garanties en matière de protection des données, qui font toujours l'objet de discussions entre le Royaume-Uni et les États-Unis, la confirmation que les autorités britanniques feront uniquement entrer cet accord en vigueur lorsqu'elles estimeront que son application est conforme aux obligations juridiques qui y figurent, y compris des engagements clairs pour le respect des normes de protection des données pour toute donnée demandée au titre de cet accord (considérant 153 du projet de décision); les situations dans lesquelles les données sont transférées depuis l'Union vers le Royaume-Uni dans le cadre de ce projet de décision, et le fait qu'une «connexion avec les îles britanniques» subsisterait toujours et que toute exploitation de réseaux informatiques visant de telles données devrait dès lors être soumise à l'exigence de mandat obligatoire visée à l'article 13, paragraphe 1, de l'IPA de 2016 (considérant 206 du projet de décision); et les exemples de finalités opérationnelles prévues (considérant 216 et note de bas de page 369 du projet de décision).

[17] Voir l'arrêt du 6 octobre 2015 dans l'affaire C-362/14, *Maximillian Schrems/Data Protection Commissioner*, ECLI:EU:C:2015:650, points 73 et 74 (ci-après l'«arrêt *Schrems I*») .

sur ce traitement et la supervision par des organes indépendants. Toutefois, les règles sur la protection des données ne sont efficaces que si elles sont applicables et suivies en pratique. Il convient donc de tenir compte non seulement du contenu des règles applicables aux données personnelles transférées vers un pays tiers ou vers une organisation internationale, mais également du système mis en place afin de garantir l'effectivité de ces règles. Des mécanismes d'application efficaces sont essentiels pour assurer l'effectivité des règles sur la protection des données[18].

## 2.3. Commentaires généraux et inquiétudes

### 2.3.1. Engagements internationaux pris par le Royaume-Uni

48. En vertu de l'article 45, paragraphe 2, point c), du RGPD, et des critères de référence pour l'adéquation dans le cadre du RGPD[19], lorsqu'elle évalue le caractère adéquat du niveau de protection d'un pays tiers, la Commission européenne tient compte, entre autres, des engagements internationaux pris par le pays tiers ou d'autres obligations découlant de la participation du pays tiers à des systèmes multilatéraux ou régionaux, en particulier en ce qui concerne la protection des données à caractère personnel, ainsi que de l'application de ces obligations. Il y a en outre lieu de prendre en considération l'adhésion du pays tiers à la convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ci-après la «convention 108»)[20] et à son protocole additionnel[21].

49. **À cet égard, l'EDPB se félicite du fait que le Royaume-Uni ait adhéré à la CEDH et relève de la juridiction de la CouEDH. Le Royaume-Uni a également adhéré à la convention 108 et à son protocole additionnel, a signé la convention 108+[22] en 2018 et travaille actuellement à sa ratification.**

### 2.3.2. Éventuelle divergence future du cadre du Royaume-Uni relatif à la protection des données

50. Comme indiqué au considérant 281 du projet de décision, la Commission européenne doit tenir compte du fait qu'avec la fin de la période de transition prévue dans l'accord de retrait[23], le Royaume-Uni administre, applique et exécute son propre régime de protection des données, et dès que la disposition transitoire au titre de l'article FINPROV.10A de l'accord de commerce et de coopération UE-Royaume-Uni[24] cesse de s'appliquer, cela pourrait notamment impliquer des modifications du cadre relatif à la protection des données examiné dans le projet de décision, ainsi que d'autres évolutions pertinentes.

---

[18] Voir WP 254 rev.01, p. 2.
[19] Voir WP 254 rev.01, p. 2.
[20] Voir la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, convention 108, 28 janvier 1981.
[21] Voir le protocole additionnel à la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données, ouvert à la signature le 8 novembre 2001.
[22] Voir le protocole modifiant la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (la «convention 108+»), 18 mai 2018.
[23] Voir l'accord sur le retrait du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord de l'Union européenne et de la Communauté européenne de l'énergie atomique (JO L 029 du 31.1.2020, p. 7).
[24] Voir l'accord de commerce et de coopération entre l'Union européenne et la Communauté européenne de l'énergie atomique, d'une part, et le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, d'autre part (JO L 444 du 31.12.2020, p. 14).

51. Aussi la Commission européenne a-t-elle décidé d'inclure une clause de limitation dans le temps dans son projet de décision[25], en vertu de laquelle la décision expirera quatre ans après son entrée en vigueur.

52. Il importe de noter que la possibilité offerte aux ministres britanniques et au secrétaire d'État du Royaume-Uni d'adopter des dispositions d'application après la fin de la période de transition pourrait à l'avenir donner lieu à une divergence considérable entre le cadre du Royaume-Uni relatif à la protection des données et celui de l'Union.

53. En effet, le gouvernement britannique a fait part de son intention de concevoir des politiques distinctes et indépendantes dans le domaine de la protection des données, ce qui pourrait entraîner une divergence par rapport à la législation de l'Union sur la protection des données[26]. Il a également l'intention d'inclure les aspects relatifs aux données à caractère personnel dans les accords commerciaux[27], pratique qui risque d'abaisser le niveau de protection des données à caractère personnel garanti par le Royaume-Uni[28].

54. Enfin, outre le fait que le Royaume-Uni n'est plus lié par la jurisprudence de la CJEU depuis la fin de la période de transition, il se pourrait que les arrêts déjà rendus par la CJUE, réputés maintenus dans le cadre juridique britannique, ne soient plus contraignants à l'égard du Royaume-Uni, en particulier

---

[25] Voir l'article 4 du projet de décision. Voir également le considérant 282 du projet de décision.

[26] La stratégie nationale du Royaume-Uni en matière de données (dernière version datant du 9 décembre 2020, https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy) inclut la mission suivante: «*Défendre les flux internationaux de données. Les flux de données transfrontalières sous-tendent les opérations commerciales, les chaînes d'approvisionnement et les échanges mondiaux, stimulant ainsi la croissance partout dans le monde. Ils jouent également un rôle sociétal plus large. Le transfert de données à caractère personnel garantit que les personnes touchent leur salaire et leur permet de communiquer à distance avec celles et ceux qui leur sont chers. Et, comme l'a montré la pandémie de coronavirus, le partage de données sanitaires peut contribuer à la recherche scientifique, vitale, sur les maladies, tout en rassemblant la réponse des pays face aux urgences sanitaires mondiales.* ***Ayant quitté l'Union européenne, le Royaume-Uni se fera le champion des avantages que peuvent fournir les données.*** *Nous encouragerons les bonnes pratiques au niveau national et travaillerons main dans la main avec des partenaires internationaux* ***pour veiller à ce que les données ne soient pas limitées de manière inappropriée par les frontières nationales et par des régimes réglementaires fragmentés****, de manière à pouvoir exploiter leur plein potentiel.»* (caractères gras ajoutés).

[27] Ibid.: «*Faciliter les flux de données transfrontaliers:* ***Nous œuvrerons à l'échelle mondiale pour éliminer les obstacles inutiles aux flux de données internationaux. Nos négociations commerciales comprendront des dispositions ambitieuses en matière de données*** *et nous utiliserons notre siège, dorénavant indépendant, au sein de l'Organisation mondiale du travail pour exercer une influence positive sur les règles commerciales relatives aux données.* ***Nous supprimerons les obstacles aux transferts internationaux de données*** *qui soutiennent la croissance et l'innovation, y compris en développant la capacité du Royaume-Uni à mettre en œuvre des mécanismes nouveaux et innovants pour les transferts internationaux de données. Nous travaillerons également avec nos partenaires du G20 à assurer l'interopérabilité des régimes nationaux de données afin de réduire au minimum les frictions lors des transferts de données entre différents pays*». (caractères gras ajoutés).

[28] Voir la résolution du Parlement européen du 12 décembre 2017 intitulée «*Vers une stratégie pour le commerce numérique*» [2017/2065(INI)], section V, dans laquelle il est souligné que «*la protection des données à caractère personnel n'est pas négociable dans les accords commerciaux [de l'Union]*», disponible à l'adresse suivante: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0488_FR.pdf. Voir également la résolution du Parlement européen du 25 mars 2021 concernant le rapport d'évaluation de la Commission sur la mise en œuvre du règlement général sur la protection des données deux ans après son entrée en application, article 28: *«soutient la pratique de la Commission européenne qui consiste à traiter la protection des données et les flux de données à caractère personnel séparément des accords commerciaux»*, https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_FR.html.

puisque le pays a la possibilité de modifier le droit conservé de l'Union à l'issue de la période de transition et que sa juridiction suprême n'est pas tenue de suivre la jurisprudence de l'Union conservée[29].

55. **Considérant les risques d'une possible déviation du cadre du Royaume-Uni relatif à la protection des données de l'acquis de l'Union à l'issue de la période de transition, l'EDPB salue la décision de la Commission européenne d'introduire dans le projet de décision une clause de limitation dans le temps de quatre ans. L'EDPB souhaite néanmoins souligner l'importance du rôle de suivi joué par la Commission européenne à cet égard[30]. En effet, à partir de l'entrée en vigueur de la décision d'adéquation visant le Royaume-Uni, la Commission européenne devrait suivre de manière continue et permanente toutes les évolutions pertinentes au Royaume-Uni susceptibles d'avoir des répercussions sur le niveau de protection substantiellement équivalent des données à caractère personnel transférées au titre de ladite décision. En outre, si, après l'adoption de la décision d'adéquation, la Commission européenne reçoit des informations indiquant que le Royaume-Uni ne garantit plus un niveau de protection adéquat, elle devrait prendre les mesures nécessaires en suspendant, modifiant ou abrogeant la décision d'adéquation, selon les circonstances.**

56. De son côté, l'EDPB mettra tout en œuvre pour informer la Commission de toute mesure pertinente prise par les autorités de l'État membre chargées du contrôle de la protection des données (ci-après les «autorités de contrôle»), dans le secteur commercial comme dans le secteur public, et en particulier en ce qui concerne les plaintes déposées par des personnes concernées dans l'EEE relatives au transfert de données à caractère personnel depuis l'EEE vers le Royaume-Uni.

# 3. ASPECTS GÉNÉRAUX DE LA PROTECTION DES DONNÉES

## 3.1. Principes généraux

57. Le chapitre 3 des critères de référence pour l'adéquation dans le cadre du RGPD est consacré aux «principes généraux». Ces principes doivent faire partie intégrante du système d'un pays tiers pour que le niveau de protection des données puisse être considéré comme substantiellement équivalent à celui garanti dans l'Union. L'EDPB reconnaît que le Royaume-Uni n'a pas de constitution codifiée, en ce sens qu'il n'existe pas de document unique qui expose ses règles fondamentales en matière de gouvernance. Cependant, le droit au respect de la vie privée et familiale (et, dans ce cadre, le droit à la protection des données) et le droit à accéder à un tribunal impartial[31] figurent dans la loi britannique de 1998 sur les droits de l'homme (Human Rights Act 1998), et la valeur constitutionnelle de ce texte a été reconnue par les juridictions britanniques. En effet, la loi britannique de 1998 sur les droits de l'homme incorpore les droits énoncés dans la CEDH[32]. En outre, il importe de souligner que cette loi dispose que toute action des autorités publiques doit être compatible avec la CEDH[33].

58. Outre les différences structurelles et formelles entre la législation du Royaume-Uni et la législation de l'Union, l'EDPB remarque, comme on pouvait s'y attendre, que l'approche britannique en matière de protection des données est semblable à celle l'Union; en effet, jusqu'au 31 janvier 2020, le

[29] Voir les articles 3 à 6 de la loi de 2018 sur l'Union européenne (retrait).
[30] Voir l'article 45, paragraphe 4, du RGPD.
[31] Voir les articles 6 et 8 de la CEDH (annexe 1 de la loi de 1998 sur les droits de l'homme).
[32] Pour de plus amples informations, voir les considérants 8 à 10 du projet de décision.
[33] Voir l'article 6 de la loi britannique de 1998 sur les droits de l'homme.

Royaume-Uni était membre de l'Union européenne. De nombreux principes généraux sont ainsi alignés sur ceux du RGPD, et offrent dès lors un niveau de protection substantiellement équivalent à celui assuré par l'Union. L'EDPB a décidé de ne pas pousser plus avant son analyse concernant les principes généraux alignés sur la législation de l'Union, et se déclare satisfait de l'analyse reprise par la Commission européenne dans son projet de décision. Ces principes généraux sont par exemple les suivants: des concepts (par exemple «données à caractère personnel»; «traitement des données à caractère personnel»; «responsable du traitement des données»), les fondements du traitement loyal et licite pour des finalités légitimes, la limitation des finalités, la qualité et la proportionnalité des données, la conservation, la sécurité et la confidentialité des données, la transparence, les catégories particulières de données, la vente directe et la prise de décision automatisée et le profilage. L'EDPB note également que le RGPD britannique et la DPA de 2018 incluent des principes généraux qui dépassent les exigences des critères de référence pour l'adéquation dans le cadre du RGPD et reflètent les principes repris dans le RGPD, ce qui augmente par conséquent le niveau de protection garanti par le Royaume-Uni. Ces principes généraux sont liés, par exemple, aux notifications de violation de données à caractère personnel, au délégué à la protection des données, aux analyses d'impact relatives à la protection des données, à la protection des données dès la conception et à la protection des données par défaut.

59. Cependant, comme évoqué dans l'introduction, l'EDPB souhaite dans le présent avis traiter plus particulièrement certains points qui le préoccupent et s'agissant desquels il entend demander des précisions à la Commission européenne.

#### 3.1.1. Le droit d'accès, de rectification, d'effacement et d'opposition

60. La «dérogation concernant l'immigration» visée à la **partie 1**, paragraphe 4 de **l'annexe 2 de la DPA de 2018** autorise les responsables du traitement intervenant dans le cadre du «contrôle de l'immigration» à ne pas respecter certains droits des personnes concernées prévus par la DPA de 2018 dès lors que ce respect serait susceptible de «*nuire au maintien d'un contrôle efficace de l'immigration*» ou à «*la détection d'activités qui pourraient nuire au maintien d'un contrôle efficace de l'immigration, ou aux enquêtes en la matière*».

61. Comme l'a reconnu la Commission européenne dans son projet de décision[34] et l'a évoqué la commission des libertés civiles, de la justice et des affaires intérieures (commission LIBE) du Parlement européen dans son avis sur la conclusion, au nom de l'Union, de l'accord de commerce et de coopération entre l'Union européenne et la Communauté européenne de l'énergie atomique, d'une part, et le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, d'autre part[35], cette

[34] Voir les considérants 62 à 65 du projet de décision.

[35] À propos de la **formulation large** de la dérogation concernant l'immigration, voir l'avis de la commission des libertés civiles, de la justice et des affaires intérieures sur la conclusion, au nom de l'Union, de l'accord de commerce et de coopération entre l'Union européenne et la Communauté européenne de l'énergie atomique, d'une part, et le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, d'autre part, et de l'accord entre l'Union européenne et le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord relatif aux procédures de sécurité pour l'échange d'informations classifiées et leur protection [2020/0382(NLE)] du 5 février 2021, https://www.europarl.europa.eu/doceo/document/LIBE-AL-680848_FR.pdf, article 10: *«rappelle à cet égard les résolutions du Parlement de février et de juin 2020, qui soulignent la **dérogation large et générale** pour le traitement des données à caractère personnel à des fins d'immigration prévue par la loi britannique sur la protection des données»* et article 11: *«estime que la dérogation **large et générale** pour le traitement des données à caractère personnel à des fins d'immigration prévue par la loi britannique sur la protection des données [...] doit être modifiée avant qu'une décision d'adéquation valable ne puisse être prise;»* (caractères gras ajoutés).

dérogation est **formulée en termes «larges»**. Elle s'applique aux droits suivants: droit d'être informé, droit d'accès, droit à l'effacement, droit à la limitation du traitement et droit d'opposition.

62. Il importe en outre de souligner que cette dérogation s'applique également lorsqu'un responsable du traitement (responsable 1) ne collecte pas des données à caractère personnel à des fins de contrôle de l'immigration, mais qu'il les met néanmoins à la disposition d'un autre responsable du traitement (responsable 2) qui, lui, ces données à caractère personnel à des fins de contrôle de l'immigration [par exemple le Home Office (le ministère de l'intérieur britannique)][36].

63. Dans *l'affaire Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin) (3 octobre 2019)*, les demandeurs contestent la légalité de la dérogation concernant l'immigration au motif qu'elle n'était ni conforme à l'article 23 du RGPD ni compatible avec les droits garantis aux articles 7 et 8 de la charte de l'Union relatifs au respect de la vie privée et à la protection des données à caractère personnel. La High Court of England and Wales (la Haute cour d'Angleterre et du pays de Galles, ci-après la «High Court») a examiné la légalité de la dérogation concernant l'immigration visée à l'annexe 2, partie 1, paragraphe 4, de la DPA de 2018 et a conclu à sa légalité.

64. La High Court a notamment estimé que:

- *«[...] la dérogation concernant l'immigration est tout simplement une "question importante d'intérêt public" et poursuit un objectif légitime. [...]»*, point 30;
- *«la dérogation concernant l'immigration satisfait aux exigences que doit respecter une mesure pour être "conforme à la loi".* […]*»*, point 38;
- *«la dérogation ne peut être appliquée que si et dans la mesure où le respect des "dispositions concernées du RGPD" **est susceptible de nuire** au maintien d'un contrôle efficace de l'immigration ou à la détection des activités qui pourraient nuire au maintien d'un contrôle efficace de l'immigration, ou aux enquêtes en la matière. L'expression "est susceptible de nuire", dans le cadre de la Data Protection Act 1998 (qui a précédé la DPA de 2018), a été interprétée telle qu'elle signifie "une probabilité très élevée que préjudice soit porté à l'intérêt public. Le*

[36] Voir l'exemple qui figure dans le «Guide du règlement général sur la protection des données (RGPD)» de l'ICO du 1er janvier 2021, p. 307 (caractères gras ajoutés): *«Une organisation privée (responsable du traitement 1) porte à l'attention du Home Office (responsable du traitement 2) un employé supposé avoir présenté de faux documents pour prouver son identité et ses compétences pour obtenir un emploi. L'employeur communique les informations pertinentes au Home Office. Le droit de la personne à savoir que ses données à caractère personnel ont été transmises au Home Office est limité dans la mesure où le lui faire savoir pourrait nuire à l'enquête.*
*Dès lors, **rien n'oblige l'employeur à informer la personne que ses données ont été communiquées au Home Office** et le **Home Office** n'est pas non plus obligé d'envoyer à la personne concernée une déclaration de confidentialité l'informant qu'il traite ses données à caractère personnel. Cette dérogation s'applique dans la même mesure aux deux responsables du traitement.*
*Cependant, l'employé demande une copie de ses données à caractère personnel au Home Office qui enquête à présent sur lui. Le **Home Office peut s'appuyer sur la dérogation** pour conserver une partie des données de l'employé si la communication de celles-ci était susceptible de nuire à l'enquête. Si l'employé venait à présenter une demande similaire à son employeur, **celui-ci pourrait également appliquer la dérogation** dans la même mesure.»*
En d'autres termes, comme cela est précisé à la page 300: *«Dans la majorité des cas, le Home Office, ou l'une de ses agences ou l'un de ses sous-traitants, sera le responsable du traitement qui applique cette dérogation. Cependant, il convient de noter que l'application de cette dérogation n'est pas uniquement limitée au Home Office. Elle peut également servir à d'autres responsables du traitement comme des employeurs, des universités et la police, qui assurent la liaison avec le Home Office sur les questions d'immigration.»*

*degré de risque doit être tel qu'il 'peut très bien' exister un préjudice pour ces intérêts, même si le risque est loin d'être plus probable qu'improbable" [...].»*, point 39 (caractères gras ajoutés).

65. Il convient de faire remarquer qu'à la connaissance de l'EDPB, ce jugement n'est pas définitif et qu'un recours a été introduit.

66. Comme il est précisé dans les lignes directrices de l'EDPB sur les limitations au titre de l'article 23 du RGPD (ci-après «les lignes directrices sur l'article 23 du RGPD»)[37] *«[...] dans le cadre du RGPD, les limitations sont* ***prévues par une mesure législative****, portent sur un* ***nombre limité de droits des personnes concernées et/ou d'obligations du responsable du traitement*** *énumérées à l'article 23 du RGPD,* ***respectent l'essence*** *des libertés et droits fondamentaux en question, sont* ***une mesure nécessaire et proportionnée*** *dans une société démocratique et garantissent l'un des motifs visés à l'article 23, paragraphe 1, du RGPD [...]»*[38].

67. L'EDPB rappelle également que le considérant 41 du RGPD précise que *«[l]orsque le présent règlement fait référence à* ***une base juridique ou à une mesure législative****, cela ne signifie pas nécessairement que l'adoption d'un acte législatif par un parlement est exigée, sans préjudice des obligations prévues en vertu de l'ordre constitutionnel de l'État membre concerné. Cependant, cette base juridique ou cette mesure législative devrait être* ***claire et précise et son application devrait être prévisible pour les justiciables****, conformément à la jurisprudence de la Cour de justice de l'Union européenne [...] et de la Cour européenne des droits de l'homme»* (caractères gras ajoutés).

68. Même si la CouEDH a précisé que *«[p]ar ailleurs, en ce qui concerne l'expression "prévue par la loi" figurant aux articles 8 à 11 de la convention, la Cour rappelle avoir toujours entendu le terme "loi" dans son acception "matérielle" et non "formelle"; elle y a inclus à la fois du "droit écrit", comprenant aussi bien des textes de rang infralégislatif que des actes réglementaires pris par un ordre professionnel, par délégation du législateur, dans le cadre de son pouvoir normatif autonome et le "droit non écrit". La "loi" doit se comprendre comme englobant le texte écrit et* ***le "droit élaboré" par les juges»***[39], les lignes directrices sur l'article 23 du RGPD rappellent que *«selon la jurisprudence de la CEDH, toute* ***mesure législative*** *adoptée sur la base de l'article 23, paragraphe 1, du RGPD doit, notamment,* ***être conforme aux exigences spécifiques visées à l'article 23, paragraphe 2, du RGPD****. L'article 23, paragraphe 2, du RGPD prévoit que les mesures législatives qui limitent les droits des personnes concernées et les obligations du responsable du traitement contiennent, le cas échéant,* ***des dispositions spécifiques relatives à plusieurs critères énumérés ci-dessous****. En règle générale, toutes les exigences exposées ci-après* ***devraient être comprises dans la mesure législative*** *qui impose des limitations au titre de l'article 23 du RGPD*»[40].

---

[37] Voir les lignes directrices 10/2020 de l'EDPB sur les limitations au titre de l'article 23 du RGPD, version 1.0, adoptées le 15 décembre 2020, actuellement en cours de finalisation à l'issue d'une consultation publique, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-102020-restrictions-under-article-23_en.

[38] Voir les lignes directrices sur l'article 23 du RGPD, paragraphe 9, p. 5.

[39] Voir l'arrêt de la CouEDH du 14 septembre 2010 dans l'affaire *Sanoma Uitgevers B.V. c. Pays-Bas*, ECLI:CE:ECHR:2010:0914JUD003822403, point 83 (caractères gras et soulignement ajoutés).

[40] Voir les lignes directrices sur l'article 23 du RGPD, paragraphes 45 et 46, p. 11. Conformément à l'article 52, paragraphe 3, de la charte de l'Union, *«[d]ans la mesure où la présente charte contient des droits correspondant à des droits garantis par la Convention de sauvegarde des droits de l'Homme et des libertés fondamentales, leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention. Cette disposition ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue»*. En ce qui concerne la notion de «**prévue par la loi**» dont il est question à l'article 52, paragraphe 1, de la charte de

69. On remarque à cet égard que la **dérogation concernant l'immigration** elle-même **ne spécifie pas les éléments suivants visés à l'article 23, paragraphe 2, du RGPD**:

- «d) [les] garanties destinées à prévenir les abus ou l'accès ou le transfert illicites»;
- «e) [le] responsable du traitement ou [les] catégories de responsables du traitement»[41];
- «g) [les] risques pour les droits et libertés des personnes concernées»;
- «h) [le] droit des personnes concernées d'être informées de la limitation, à moins que cela risque de nuire à la finalité de la limitation».

70. Le «Guide du règlement général relatif à la protection des données (RGPD)» de l'ICO[42], qui comprend un chapitre consacré à la «dérogation concernant l'immigration», apporte des précisions sur la dérogation concernant l'immigration, mais ne **peut pas** en soi établir des règles contraignantes qui la compléteraient. En outre, la question de la «qualité de la loi» se pose avec une grande acuité au vu de l'importance des droits qui font l'objet de limitations et de l'étendue de la dérogation[43].

---

l'Union, il convient d'utiliser les critères dégagés par la CEDH, comme plusieurs avocats généraux de la CJUE l'ont préconisé dans leurs conclusions: voir, par exemple, les conclusions dans les affaires jointes C-203/15 et C-698/15, *Tele2 Sverige AB*, ECLI:EU:C:2016:572, points 137 à 154, et dans l'affaire C-70/10, *Scarlet Extended*, ECLI:EU:C:2011:255, points 88 à 114. Il est ainsi possible de faire référence, entre autres, à l'arrêt de la CouEDH dans l'affaire *Weber et Saravia c. Allemagne*, point 84: *«La Cour rappelle que les mots "**prévue par la loi**", au sens de l'article 8 § 2 [de la CEDH], veulent d'abord que la mesure incriminée ait une base en **droit interne**, mais ils ont trait aussi à la **qualité de la loi** en cause: ils exigent l'accessibilité de celle-ci à la personne concernée, qui de surcroît doit pouvoir en prévoir les conséquences pour elle, et sa compatibilité avec la prééminence du droit.»* (caractères gras ajoutés).
Voir également le considérant 41 du RGPD: *«Cette base juridique ou cette mesure législative devrait être **claire** et **précise** et son application devrait être **prévisible pour les justiciables**, conformément à la jurisprudence de la Cour de justice de l'Union européenne [...] et de la Cour européenne des droits de l'homme»* (caractères gras ajoutés).

[41] Voir l'affaire devant la High Court, susmentionnée, point 54: *«Je ne vois rien d'illégal au fait que **tous les responsables du traitement** qui traitent des données aux fins précisées puissent invoquer la dérogation concernant l'immigration. Comme l'ont fait remarquer les défendeurs, sans le paragraphe 4, points 3 et 4, la dérogation concernant l'immigration serait nulle dans les cas où les données sont obtenues auprès de tiers [comme une autorité locale ou le service de la fiscalité et des douanes (Her Majesty's Revenue and Customs)] aux fins de maintien d'un contrôle effectif de l'immigration.»* (caractères gras ajoutés), ce qui confirme l'application **généralisée** des limitations.

[42] «Guide du règlement général relatif à la protection des données (RGPD)» de l'ICO du 1er janvier 2021, p. 299 à 307.

[43] Voir le point 57 de l'affaire devant la High Court, susmentionnée: *«M. Knight m'informe que le commissaire apporte les dernières touches aux orientations concernant la dérogation, mais celles-ci n'auront de statut "ayant valeur de loi" que dans la mesure où elles sont émises en vertu des pouvoirs du commissaire au titre de l'article 57, paragraphe 1, du RGPD. Elles n'auront pas de statut juridique au titre de la loi DPA de 2018.»*
Le raisonnement qui sous-tend l'introduction d'orientations juridiquement contraignantes, encouragée par l'ICO, est évoqué notamment aux points 56 à 60 de l'arrêt:
*«56. J'en arrive enfin à la proposition du commissaire selon laquelle en l'absence d'orientations d'accompagnement ayant valeur de loi pour offrir des garanties quant à la signification et à l'application de la dérogation concernant l'immigration, celle-ci ne constituerait pas une mise en œuvre proportionnée de l'article 23, paragraphe 1, du RGPD. M. Knight affirme que la disposition est proportionnée si elle est complétée par de telles orientations.*
*57. «M. Knight m'informe que le commissaire apporte les dernières touches aux orientations concernant la dérogation, mais celles-ci n'auront de statut "ayant valeur de loi" que dans la mesure où elles sont émises en vertu des pouvoirs du commissaire au titre de l'article 57, paragraphe 1, du RGPD. Elles n'auront pas de statut*

71. A fortiori, le «**critère du préjudice**» n'énonce pas les garanties destinées à prévenir les abus ou l'accès ou le transfert illicites et devant être mises en place par le Home Office, par exemple.

72. Au vu de ce qui précède, l'EDPB fait observer que des précisions supplémentaires sur l'application de la dérogation concernant l'immigration sont nécessaires.

73. En outre, l'EDPB note l'absence d'un instrument juridiquement contraignant qui préciserait si la dérogation concernant l'immigration doit être considérée comme étant équivalente en substance à l'article 23 du RGPD et aux articles 7 et 8 de la charte de l'Union. Dans le même temps, l'EDPB estime que la Commission européenne devrait, en s'appuyant sur des éléments de preuve, démontrer plus en détail la nécessité et la proportionnalité du large champ d'application ratione personae de la dérogation concernant l'immigration.

---

*juridique au titre de la loi DPA de 2018. Je comprends également que le Home Office a produit un projet d'orientations internes destinées au personnel quant à la dérogation concernant l'immigration (voir point 22 ci-dessus). Dans la pratique, les orientations publiées par le commissaire ont un poids, peu importe leur base juridique. Cependant, le commissaire n'est nullement habilité à publier des orientations «contraignantes» au sens où l'entendait la High Court dans l'affaire Christian Institute (points 101 et 107). Il semble que des dispositions de législation primaire seraient requises si l'on estimait nécessaire de pouvoir disposer d'orientations quant à la dérogation concernant l'immigration, et qui jouissent du même statut que les codes de pratique actuellement visés aux articles 121 à 124 de la loi DPA de 2018.*
*58. Dans son argument en faveur de l'établissement d'orientations ayant valeur de loi, M. Knight affirme que le contexte dans lequel intervient le recours à la dérogation concernant l'immigration conditionne nécessairement les inquiétudes quant à la nécessité et à la proportionnalité de son existence et de son utilisation. Il attire l'attention sur deux points en particulier dans le contexte juridique. Premièrement, les données à caractère personnel auxquelles s'applique la dérogation concernant l'immigration sont par nature susceptibles d'inclure des données relevant d'une catégorie particulière au sens de l'article 9, paragraphe 1, du RGPD (à savoir des «données qui révèle[nt] l'origine raciale ou ethnique»). Ces données sont précisées dans le RGPD car elles requièrent un niveau de protection plus élevé (conclusions 1/15 [2019] 3 C.M.L.R.25, point 141).* Deuxièmement, le fait que le droit d'accès des personnes concernées en particulier revête une importance considérable en ce qu'il permet d'exercer les autres droits dont disposent les personnes concernées est une idée de base de la législation en matière de protection des données[voir l'arrêt de la Cour de justice *YS contre Minister voor Immigratie, Integratie en Asiel (C-141/12) ECLI:EU:C:2014:2081;[2015] 1 C.M.L.R.18, point 44*].
*59. M. Knight relève quatre points de nature pratique. Premièrement, lorsque les responsables du traitement n'expliquent pas aux personnes concernées qu'ils se sont servis d'une dérogation réglementaire, et n'en indiquent pas non plus les raisons de manière générale, la personne concernée ne saura pas que la dérogation a été mise en œuvre et ne sera dès lors pas en mesure de la contester. Deuxièmement, les personnes concernées devront notamment s'en remettre aux responsables du traitement pour ce qui est d'appliquer la dérogation avec précaution et uniquement dans la mesure où cela est nécessaire. Même si toute personne concernée a le droit d'introduire une réclamation auprès du commissaire visant l'application de la dérogation ou d'intenter une action devant les tribunaux, il est probable qu'elle ne connaisse pas ses droits et ne dispose pas des ressources financières nécessaires pour prendre des mesures juridiques, alors même que la situation requiert que des droits liés à la protection des données soient rapidement et scrupuleusement respectés. Troisièmement, en tant que personne immigrée, la personne concernée est susceptible d'être en situation de vulnérabilité. Quatrièmement, à la lumière des preuves présentées par les défendeurs quant à l'utilisation de la dérogation concernant l'immigration, il ne s'agit pas d'une question abstraite (voir point 4 ci-dessus).*
*60. M. Knight laisse entendre qu'il existe un lien étroit entre le problème de la dérogation concernant l'immigration et le raisonnement développé par la Cour dans l'affaire Christian Institute [2016] UKSC 51. Il affirme que, tout comme dans l'affaire Christian Institute, la dérogation concernant l'immigration est très large, utilise des termes non définis, applique un seuil bas, est soumise à des contrôles qui n'apparaissent pas dans la disposition et s'applique à un vaste ensemble de contextes et de droits. Contrairement à l'affaire Christian Institute, il n'existe pas de lignes directrices accessibles au public, encore moins de statut "ayant valeur de loi", devant être prises en compte, relatives à la dérogation concernant l'immigration*».

74. **Pour conclure, l'EDPB invite la Commission européenne à vérifier l'état d'avancement de la procédure dans l'affaire Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin), susmentionnée, et étant donné que le jugement n'est pas définitif (autorité de la chose jugée), à vérifier si celui-ci est confirmé ou infirmé par le jugement prononcé en appel, en tenant compte de toute évolution à cet égard, à le préciser dans la décision. L'EDPB invite également la Commission européenne à fournir des informations supplémentaires concernant la nécessité et la proportionnalité de la dérogation concernant l'immigration, notamment en ce qui concerne le large champ d'application ratione personae.**

75. **Dans le même temps, l'EDPB invite la Commission européenne à examiner plus avant si des garanties supplémentaires existent ou pourraient être envisagées dans le cadre juridique britannique, par exemple au moyen d'instruments juridiquement contraignants qui viendraient compléter la dérogation concernant l'immigration en améliorant la prévisibilité pour les personnes concernées et en renforçant les garanties destinées à celles-ci, ce qui permettrait également d'assurer une évaluation et un suivi rapides et améliorés des exigences de nécessité et de proportionnalité.**

### 3.1.2. Limitations concernant les transferts ultérieurs

76. L'article 44 du RGPD prévoit que les transferts et les transferts ultérieurs de données à caractère personnel ne peuvent avoir lieu que si le niveau de protection des personnes physiques garanti par ce règlement n'est pas compromis. Par conséquent, les données à caractère personnel transférées depuis l'EEE vers le Royaume-Uni sur la base de la décision d'adéquation doivent bénéficier d'un niveau de protection substantiellement équivalent à celui prévu par le cadre de l'Union régissant la protection des données. **Cela signifie non seulement que la législation britannique doit être «substantiellement équivalente» à la législation de l'Union en ce qui concerne le traitement des données à caractère personnel transférées vers le Royaume-Uni au titre du projet de décision, mais également que les règles applicables au Royaume-Uni concernant le transfert ultérieur de ces données à des pays tiers doivent garantir qu'un niveau de protection substantiellement équivalent continuera d'être assuré.**

77. Dès lors, il est important que tout transfert ultérieur depuis le Royaume-Uni vers un pays tiers de données à caractère personnel provenant de l'EEE soit dûment protégé par des garanties ou soit réalisé conformément aux règles relatives aux dérogations[44], afin d'assurer la continuité de la protection offerte par la législation de l'Union. **En effet, s'il s'avère impossible d'assurer une telle protection, les transferts ultérieurs des données à caractère personnel provenant de l'EEE ne devraient pas avoir lieu.**

78. L'EDPB reconnaît que le Royaume-Uni a en grande partie repris le chapitre V du RGPD dans le RGPD britannique (articles 44 à 49) et dans la DPA de 2018[45]. **L'EDPB a cependant relevé certains aspects du cadre législatif britannique concernant les transferts ultérieurs susceptibles de compromettre le niveau de protection des données à caractère personnel transférées depuis l'EEE.**

79. **Le premier élément problématique** relevé par l'EDPB porte sur la reconnaissance par le Royaume-Uni, à l'issue de la procédure prévue dans la DPA de 2018, de pays tiers, d'organisations

[44] Voir l'article 49 du RGPD britannique.
[45] Voir les articles 17A, 17B, 17C et 18 de la DPA de 2018.

internationales ou de territoires[46] comme destinataires adéquats. En effet, des transferts ultérieurs de données à caractère personnel provenant de l'EEE pourraient avoir lieu entre le Royaume-Uni et d'autres pays tiers, sur la base d'un éventuel futur règlement d'adéquation britannique[47].

80. Plus précisément, comme l'explique la Commission au considérant 77 du projet de décision, le secrétaire d'État britannique dispose du pouvoir de reconnaître qu'un pays tiers (ou un territoire ou un secteur d'un pays tiers), une organisation internationale ou une description de ce pays, de ce territoire, de ce secteur ou de cette organisation assure un niveau adéquat de protection des données à caractère personnel, et ce après consultation de l'ICO[48]. Lorsqu'il évalue le caractère adéquat du niveau de protection, le secrétaire d'État britannique doit tenir compte des mêmes éléments que ceux que la Commission européenne est tenue d'apprécier au titre de l'article 45, paragraphe 2, points a) à c), du RGPD, interprété conjointement avec le considérant 104 de ce même règlement, et la jurisprudence conservée de l'UE. Autrement dit, lors de l'évaluation du caractère adéquat du niveau de protection d'un pays tiers, le critère pertinent consistera à déterminer si le pays tiers en question assure un niveau de protection «substantiellement équivalent» à celui qui est garanti au Royaume-Uni. Tout en prenant acte de la capacité du Royaume-Uni, au titre du RGPD britannique, de reconnaître des territoires assure un niveau de protection adéquat au regard du cadre du Royaume-Uni relatif à la protection des données, l'EDPB souhaite souligner le fait que de tels territoires peuvent, à ce jour, ne pas bénéficier d'une décision d'adéquation délivrée par la Commission européenne et reconnaissant un niveau de protection «substantiellement équivalent» à celui garanti dans l'UE. Cela pourrait entraîner d'éventuels risques en ce qui concerne la protection assurée pour les données à caractère personnel transférées depuis l'EEE, notamment si, à l'avenir, le cadre du Royaume-Uni relatif à la protection des données venait à s'écarter de l'acquis de l'Union. Il convient de noter qu'en juillet 2020, l'arrêt de la CJUE dans l'affaire *Schrems II*[49], qui fait d'ores et déjà autorité, a entraîné l'invalidation de la décision relative au bouclier de protection des données des États-Unis puisque, selon la CJUE, il était impossible de considérer que le cadre juridique de ce pays fournissait un niveau de protection substantiellement équivalent à celui de l'Union. Cependant, il se pourrait que les arrêts déjà rendus par la CJUE, considérés comme une jurisprudence conservée dans le cadre juridique britannique, ne soient plus contraignants à l'égard du Royaume-Uni, en particulier puisque le pays a la possibilité de modifier le droit conservé de l'Union à l'issue de la période de transition et que sa juridiction suprême n'est pas tenue de suivre la jurisprudence de l'Union conservée[50].

81. **L'EDPB invite la Commission européenne à suivre de près le processus et les critères d'évaluation de l'adéquation mis en œuvre par les autorités britanniques vis-à-vis d'autres pays tiers, notamment en ce qui concerne les pays tiers que l'Union ne reconnaît pas comme adéquats au titre du RGPD. Lorsque la Commission européenne constate qu'un pays tiers considéré comme adéquat par le Royaume-Uni n'assure pas de niveau de protection substantiellement équivalent à celui garanti dans l'Union, l'EDPB invite la Commission européenne à prendre toutes les mesures nécessaires, par exemple modifier la décision d'adéquation visant le Royaume-Uni afin d'introduire des garanties spécifiques pour les données à caractère personnel provenant de l'EEE**

[46] Voir l'article 17A de la DPA de 2018.

[47] L'équivalent britannique d'une décision d'adéquation au titre du RGPD.

[48] Voir l'article 182, paragraphe 2, de la DPA de 2018. Voir également le protocole d'accord sur le rôle de l'ICO en lien avec les nouvelles évaluations d'adéquation britanniques, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/03/secretary-of-state-for-the-department-for-dcms-and-the-information-commissioner-sign-memorandum-of-understanding/.

[49] Voir l'arrêt *Schrems II*.

[50] Voir les articles 3 à 6 de la loi de 2018 sur l'Union européenne (retrait).

**et/ou envisager de suspendre la décision d'adéquation visant le Royaume-Uni lorsque les données à caractère personnel transférées depuis l'EEE vers le Royaume-Uni sont soumises à un transfert ultérieur vers le pays tiers en question sur la base d'un règlement d'adéquation britannique.**

82. **Le deuxième élément problématique** porte sur le réexamen à venir des décisions d'adéquation déjà existantes délivrées par la Commission européenne en vertu de la directive 95/46/CE. À la suite de ce réexamen, la Commission européenne pourrait décider que certains pays qui ont jusqu'à présent bénéficié d'une décision d'adéquation n'assurent plus un niveau de protection substantiellement équivalent au regard de la législation actuelle de l'Union et de la jurisprudence récente. Cependant, comme le prévoit l'annexe 21, paragraphe 4, de la DPA de 2018, le Royaume-Uni a déjà reconnu que ces pays assurent un niveau de protection adéquat. Bien que le secrétaire d'État britannique doive réaliser un réexamen de ces décisions d'adéquation dans un délai de quatre ans, la Commission européenne note dans son projet de décision que ces constatations d'adéquation ne cesseraient pas automatiquement d'exister si le secrétaire d'État britannique ne procédait pas à ce réexamen requis dans le délai prévu de quatre ans[51].

83. **L'EDPB invite la Commission européenne à vérifier, une fois que l'Union aura terminé son examen des décisions d'adéquation déjà existantes, si le Royaume-Uni continue d'estimer qu'un pays fournit un niveau de protection adéquat alors que l'examen réalisé par l'Union en a conclu différemment. Si tel est le cas, l'EDPB invite la Commission européenne, sur la base des considérants 277 à 280 du projet de décision, à prendre toutes les mesures appropriées afin de remédier à la situation, par exemple en modifiant la décision d'adéquation afin d'ajouter des exigences spécifiques pour les données à caractère personnel provenant de l'EEE et/ou en suspendant la décision d'adéquation si les données à caractère personnel transférées depuis l'EEE vers le Royaume-Uni sont soumises à des transferts ultérieurs vers le pays tiers en question. L'EDPB invite la Commission européenne à poursuivre cet exercice de suivi tout au long de la durée de la décision d'adéquation visant le Royaume-Uni.**

84. **Le troisième élément problématique** concerne le transfert ultérieur des données à caractère personnel provenant de l'EEE vers des pays non adéquats au moyen des outils de transfert prévus par les articles 46 et 47 du RGPD britannique. Bien que le RGPD britannique prévoie les mêmes outils de transfert que le RGPD, l'EDPB souligne qu'il est nécessaire de veiller à ce que les garanties qu'il contient assurent une protection efficace dans le pays tiers, notamment à la lumière de l'arrêt *Schrems II*.

85. Suite à l'arrêt rendu dans l'affaire *Schrems II*, dans lequel la CJUE rappelle que la protection accordée aux données à caractère personnel dans l'Union doit accompagner les données quelle que soit leur destination, l'EDPB a déjà adopté des recommandations initiales relatives à des mesures supplémentaires[52] visant à aider les exportateurs, le cas échéant, à veiller à ce que les personnes concernées bénéficient d'un niveau de protection substantiellement équivalent à celui garanti dans l'Union.

---

[51] Voir considérant 82 du projet de décision.

[52] Voir les recommandations 01/2020 de l'EDPB relatives à des mesures devant compléter 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, en cours de finalisation à l'issue d'une consultation publique, https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_fr.pdf.

86. Selon la CJUE, les exportateurs de données doivent vérifier, au cas par cas et, le cas échéant, en collaboration avec l'importateur des données dans le pays tiers, si le droit ou la pratique du pays tiers nuit à l'efficacité des garanties appropriées prévues par l'article 46 du RGPD pour les outils de transfert[53]. Si c'est le cas, les exportateurs de données devraient mettre en œuvre des mesures supplémentaires qui comblent ces lacunes de la protection et la renforcent pour atteindre le niveau requis par le droit de l'Union.

87. **L'EDPB invite la Commission européenne, afin de garantir la continuité de la protection, à introduire dans le projet de décision des garanties assurant que, lorsque des exportateurs de données au Royaume-Uni utilisent les outils de transfert prévus aux articles 46 et 47 du RGPD britannique dans le cadre de transferts ultérieurs vers d'autres pays tiers de données transférées depuis l'EEE, ces exportateurs évaluent au cas par cas le cadre de protection des données du pays tiers et, si nécessaire, prennent les mesures appropriées pour assurer le respect effectif des garanties contenues dans l'outil de transfert retenu, ainsi qu'un niveau de protection substantiellement équivalent à celui garanti dans l'Union. En l'absence de telles garanties, l'EDPB souligne que le niveau de protection substantiellement équivalent à celui assuré dans l'Union risque d'être dilué dans les transferts ultérieurs ayant lieu depuis le Royaume-Uni.**

88. **Le quatrième élément problématique** en matière de transferts ultérieurs concerne les accords internationaux conclus, ou à conclure à l'avenir, par le Royaume-Uni, et la possibilité que les autorités des pays tiers parties à ces accords puissent accéder directement aux données à caractère personnel provenant de l'EEE. En effet, l'EDPB nourrit de vives inquiétudes à l'endroit de l'accord CLOUD Act déjà conclu entre le Royaume-Uni et les États-Unis, et la Commission européenne reconnaît cet élément problématique, en soulignant que l'«*éventuelle entrée en vigueur de l'accord pourrait avoir une incidence sur le niveau de protection évalué dans la présente décision*»[54]. En effet, sur la base de cet accord, lorsqu'il sera entré en vigueur, les données à caractère personnel transférées depuis l'EEE vers le Royaume-Uni au titre du projet de décision seraient alors soumises aux dispositions de cet accord, qui établit les conditions d'accès direct des autorités des États-Unis et a une incidence sur le cadre de protection des données du Royaume-Uni, y compris sur les dispositions relatives aux transferts ultérieurs. Dès lors, le niveau de protection dont bénéficient les données transférées depuis l'EEE peut être considérablement affecté par les dispositions de l'accord conclu avec les États-Unis, qui ont une incidence sur le niveau de protection conféré à ces données. Dans ce contexte, l'EDPB observe que la Commission européenne fait référence aux explications fournies par les autorités britanniques dans le considérant 153 de son projet de décision, sans citer ni fournir de garantie ou d'engagement concrets, et sans indiquer les dispositions juridiques spécifiques du droit britannique qui donneraient effet à de telles explications.

89. L'EDPB a déjà fait part de ses inquiétudes dans une lettre adressée au Parlement européen en date du 15 juin 2020[55]. L'EDPB soulignait que, au vu de «*l'acquis de l'Union dans le domaine de la protection des données à caractère personnel, et notamment le RGPD et la directive sur les autorités répressives*», il émettait des réserves quant à la question de savoir si les garanties contenues dans l'accord pour l'accès aux données à caractère personnel au Royaume-Uni s'appliqueraient dans certaines circonstances impliquant des obligations de divulgation aux États-Unis, et si ces garanties

[53] Voir l'arrêt *Schrems II*, point 134.

[54] Voir considérant 153 du projet de décision.

[55] Voir la réponse de l'EDPB aux députés au Parlement européen M^me^ Sophie in't Veld et M. Moritz Körner sur l'accord entre les États-Unis et le Royaume-Uni en vertu de la loi CLOUD des États-Unis (US Cloud Act), adoptée le 15 juin 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf.

étaient suffisantes au regard des normes de l'Union, de sorte à ne pas compromettre le niveau de protection garanti dans l'Union.

90. En outre, les dispositions de l'accord CLOUD Act peuvent avoir une incidence considérable sur les conditions de fond et de forme régissant l'accès direct des autorités des États-Unis aux données à caractère personnel détenues par les responsables du traitement ou par les sous-traitants au Royaume-Uni, ce qui a un impact sur le niveau de protection garanti par le droit britannique. Afin de fournir un niveau de protection substantiellement équivalent à celui garanti par le droit de l'Union, il est par exemple «*crucial que les garanties prévues au titre d'un tel accord comprennent une autorisation judiciaire préalable obligatoire, à titre de garantie essentielle pour l'accès aux métadonnées et aux données relatives au contenu. Sur la base de son évaluation préliminaire, l'EDPB, tout en notant que l'accord fait référence à l'application du droit national, n'est pas parvenu à dégager des dispositions claires en ce sens dans l'accord conclu entre le Royaume-Uni et les États-Unis*»[56].

91. Bien que la Commission européenne souligne que les données obtenues en vertu de cet accord bénéficieraient de protections équivalentes aux garanties spécifiques prévues dans l'accord UE-USA sur la protection des données à caractère personnel, l'EDPB s'inquiète de savoir si l'incorporation de ces garanties dans l'accord CLOUD Act par une simple référence s'appliquant mutatis mutandis suffirait à satisfaire aux critères de règles claires, précises et accessibles concernant l'accès aux données, ou si elle donnerait lieu à une consécration suffisante de ces garanties, les rendant effectives et opposables en droit britannique.

92. **L'EDPB recommande donc à la Commission européenne de préciser de quelle manière et sur la base de quels instruments juridiques des protections équivalentes aux garanties spécifiques prévues dans l'accord UE-USA sur la protection des données à caractère personnel produiront leurs effets et acquerront un caractère contraignant en droit britannique.**

93. L'EDPB fait également observer que les dispositions de l'accord CLOUD Act, lues conjointement avec l'article 3 de la loi CLOUD des États-Unis[57], soulèvent des questions quant à l'application réelle des garanties prévues dans l'accord en ce qui concerne l'accès des autorités répressives des États-Unis à des données à caractère personnel au Royaume-Uni traitées par des fournisseurs de services de communication électronique ou de services d'informatique à distance (ci-après les «FSCI») relevant de la compétence des États-Unis. En effet, dans le cas où un FSCI situé au Royaume-Uni doit se soumettre au droit des États-Unis (par exemple, s'il s'agit d'une filiale d'une entreprise des États-Unis), il reste à déterminer si les autorités des États-Unis seront tenues d'invoquer l'accord CLOUD Act pour obtenir ces données. Alors que la Commission européenne souligne qu'«*une attention particulière sera portée à l'application et à l'adaptation des protections de l'accord UE-USA sur la protection des données à caractère personnel au type spécifique de transfert visé par l'accord entre le Royaume-Uni et les États-Unis*», l'EDPB souligne que, sur la base de son évaluation préliminaire, il s'avère impossible de déterminer clairement si les garanties inscrites dans l'accord CLOUD Act, et, donc, celles prévues dans l'accord UE-USA sur la protection des données à caractère personnel, s'appliqueraient, le cas échéant, à l'ensemble des demandes d'accès aux données au Royaume-Uni formulées par les autorités des États-Unis au titre de la loi CLOUD des États-Unis.

94. À l'avenir, il se peut que le Royaume-Uni conclue d'autres accords ou engagements internationaux avec des pays tiers, qui s'appliqueraient aux données à caractère personnel transférées depuis l'EEE

[56] Voir la lettre de l'EDPB susmentionnée.
[57] Voir la loi CLOUD des États-Unis, https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.

vers le Royaume-Uni au titre du projet de décision[58]. En fonction des dispositions de ces accords et de l'application de clauses de garantie spécifiques, ces accords internationaux, en affectant le cadre britannique de la protection des données, pourraient également avoir un impact considérable sur les conditions de fond et de forme régissant l'accès des autorités des pays tiers à des données à caractère personnel au Royaume-Uni. C'est tout particulièrement le cas du projet de deuxième protocole additionnel à la convention du Conseil de l'Europe sur la cybercriminalité (ci-après la «Convention de Budapest»), qui fait actuellement l'objet de négociations entre les parties à cette convention, dont certaines ne sont pas membres de l'Union. En effet, le projet de protocole inclut des clauses qui peuvent être activées à la discrétion des parties, notamment en ce qui concerne l'autorisation d'accorder ou non l'accès aux données relatives aux contenus. Alors que tous les États membres activeraient ces clauses conformément aux règles de l'Union concernant la protection des données, aucune garantie n'a été fournie en ce qui concerne le Royaume-Uni, qui pourrait s'écarter de manière considérable du niveau de protection alors assuré dans l'Union. L'accord entre le Royaume-Uni et le Japon visant un partenariat économique global (Comprehensive Economic Partnership Agreement, ci-après l'accord «CEPA»)[59], premier accord commercial post-Brexit signé par le Royaume-Uni, entré en vigueur le 1er janvier 2021,[60] qui comprend des dispositions concernant les données à caractère personnel[61], constitue un autre exemple des points problématiques exposés précédemment. L'EDPB fait en outre observer que le Royaume-Uni a également indiqué, le 1er février 2021, qu'il avait demandé à rejoindre l'accord de partenariat transpacifique global et progressiste (Comprehensive and Progressive Trans-Pacific Partnership, «PTPGP»), qui intègre l'accord de partenariat transpacifique (ci-après l'«accord PTP»)[62].

95. L'EDPB fait observer que, à l'exception de l'accord CLOUD Act, le projet de décision ne traite pas des accords internationaux susmentionnés.

96. **L'EDPB invite la Commission:**

- **À examiner les interactions entre le cadre du Royaume-Uni relatif à la protection des données et ses engagements internationaux, au-delà de l'accord CLOUD Act, notamment afin de garantir la continuité du niveau de protection en cas de transferts ultérieurs vers d'autres pays tiers de données à caractère personnel transférées depuis l'EEE vers le Royaume-Uni sur la base d'une décision d'adéquation, et, en permanence, à assurer un suivi et à prendre des mesures, s'il y a lieu, en cas de conclusion d'autres accords internationaux entre le Royaume-Uni et des pays tiers qui risqueraient de compromettre le niveau de protection des données à caractère personnel garanti dans l'Union.**

---

[58] Voir la section 2.3.3. ci-dessus.

[59] Voir Royaume-Uni/Japon: Accord pour un partenariat économique global [CS Japan nº 1/2020], https://www.gov.uk/government/publications/ukjapan-agreement-for-a-comprehensive-economic-partnership-cs-japan-no12020.

[60] Voir les lignes directrices du gouvernement britannique sur les accords commerciaux conclus par le Royaume-Uni avec des pays non membres de l'Union, https://www.gov.uk/guidance/uk-trade-agreements-with-non-eu-countries.

[61] En application de l'article 8.80, paragraphe 5, de l'accord CEPA, les parties s'engagent à encourager la mise au point de mécanismes afin de faciliter la compatibilité entre leurs différentes approches juridiques de la protection des données (à caractère personnel). Conformément à l'article 8.84, les parties s'engagent à ne pas interdire ni limiter le transfert transfrontière d'informations par voie électronique, y compris d'informations personnelles, lorsque cela relève des activités d'une personne couverte au sens de l'accord CEPA.

[62] En application de l'article 14.11, paragraphe 2, de l'accord PTP, chaque partie autorise le transfert transfrontière d'informations par voie électronique, y compris d'informations personnelles, lorsque cela relève des activités d'une personne couverte.

- **À lui fournir les engagements écrits pris par les autorités britanniques et à déterminer les dispositions spécifiques du droit britannique en ce qui concerne l'explication de l'application et de la mise en œuvre possibles de l'accord CLOUD Act, mentionnées au considérant 153 du projet de décision.**

- **À surveiller, dans ce contexte, si, outre les garanties susceptibles d'être assurées par une mise en œuvre appropriée de l'adaptation de l'accord UE-USA sur la protection des données à caractère personnel, l'accord CLOUD Act fournit des garanties supplémentaires appropriées afin de tenir compte du degré de sensibilité des catégories de données concernées ainsi que des exigences uniques imposant que le transfert de preuves électroniques soit effectué directement par les FSCI plutôt qu'il ait lieu entre les autorités.**

- **À évaluer l'impact et les risques potentiels des dispositions relatives aux données à caractère personnel contenues dans les accords internationaux récemment signés par le Royaume-Uni, comme l'accord CEPA.**

97. **Le cinquième élément problématique** relevé porte sur l'application de dérogations au transfert de données à caractère personnel à un pays tiers. Bien que les dérogations prévues dans le RGPD britannique soient les mêmes que celles prévues par le RGPD, il importe que l'ICO applique et continue d'appliquer une interprétation de l'utilisation de ces dérogations qui soit conforme à celle de l'EDPB. Si tel n'est pas le cas, ou si le Royaume-Uni s'écarte de cette interprétation à l'avenir, le niveau de protection des données transférées depuis l'EEE vers des pays tiers via le Royaume-Uni risquerait d'être compromis.

98. **L'EDPB invite la Commission, dans le cadre de sa mission de surveillance, à vérifier spécifiquement que l'interprétation faite par le Royaume-Uni de l'utilisation des dérogations reste conforme à l'interprétation faite par l'Union. Toutefois, si le Royaume-Uni venait à adopter une interprétation différente de l'utilisation des dérogations compromettant le niveau de protection, il est crucial que la Commission européenne prenne les mesures nécessaires en modifiant la décision d'adéquation afin de veiller à ce que le niveau de protection assuré aux données à caractère personnel de l'EEE transférées au Royaume-Uni ne soit pas compromis à l'occasion du transfert ultérieur de ces données depuis le Royaume-Uni vers des pays tiers sur la base d'une interprétation différente des dérogations.**

99. **Le sixième défi**, et le dernier pour cette section, porte sur l'absence des protections prévues par l'article 48 du RGPD dans le cadre du Royaume-Uni relatif à la protection des données.

100. La Commission précise en effet dans son projet de décision que, en l'absence de règlements d'adéquation ou de garanties appropriées, un transfert ne peut avoir lieu que sur la base des dérogations prévues à l'article 49 du RGPD britannique, «*à l'exception de l'article 48 du règlement (UE) 2016/679, que le Royaume-Uni a choisi de ne pas inclure dans le RGPD britannique*».[63] L'absence d'une disposition substantiellement équivalente à l'article 48 du RGPD dans le cadre du Royaume-Uni relatif à la protection des données, s'agissant de transferts ou de divulgations, à la suite d'une décision de justice ou d'une décision d'une autorité administrative d'un autre pays tiers, peut donner naissance à une insécurité juridique quant à savoir si le niveau de protection dont bénéficient les données à caractère personnel transférées depuis l'EEE vers le Royaume-Uni en vertu du projet de décision serait substantiellement affecté.

63 Voir note de bas de page 78 du projet de décision.

101. Dans ses critères de référence pour l'adéquation dans le cadre du RGPD, l'EDPB souligne que, s'agissant des transferts ultérieurs, «*les transferts ultérieurs des données à caractère personnel par le destinataire initial du transfert original de données ne devraient être autorisés que si le nouveau destinataire* […] *est également soumis à des règles* […] *assurant un niveau de protection adéquat et suivant les instructions pertinentes lors du traitement des données pour le compte du responsable du traitement*»[64]. L'EDPB souligne également que «*le destinataire initial des données transférées depuis l'UE doit s'assurer que les garanties appropriées sont prévues pour les transferts ultérieurs de données en l'absence d'une décision d'adéquation. Ces transferts ultérieurs de données ne devraient avoir lieu qu'à des fins limitées et précises et tant que ce traitement a un fondement juridique*»[65]. Dans le cadre du chapitre V du RGPD, il convient de tenir pleinement compte de l'article 48 afin de déterminer si le cadre juridique britannique garantit un niveau de protection substantiellement équivalent à cet égard[66].

102. Dans ce contexte, l'EDPB met l'accent sur la jurisprudence de la CJUE ayant trait au risque d'abus ou d'accès et d'utilisation illicites, en affirmant notamment que «*s'agissant du niveau de protection des libertés et droits fondamentaux garanti au sein de l'Union, une réglementation de celle-ci comportant une ingérence dans les droits fondamentaux garantis par les articles 7 et 8 de la charte doit, selon la jurisprudence constante de la Cour, prévoir des règles claires et précises régissant la portée et l'application d'une mesure et imposant un minimum d'exigences, de sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement leurs données contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données. La nécessité de disposer de telles garanties est d'autant plus importante lorsque les données à caractère personnel sont soumises à un traitement automatique et qu'il existe un risque important d'accès illicite à ces données*»[67].

103. À cet égard, l'EDPB fait observer que, sur la base des informations disponibles dans le projet de décision, le cadre du Royaume-Uni relatif à la protection des données n'indique pas clairement que toute décision de justice et toute décision administrative d'un pays tiers imposant à un responsable du traitement ou à un sous-traitant de divulguer des données à caractère personnel ne peut être reconnue ou exécutoire, de quelque manière que ce soit, que si elle se fonde sur un accord international en vigueur conclu entre le pays tiers demandeur et le Royaume-Uni. L'article 48 du RGPD est une disposition essentielle du chapitre V de ce règlement, car il exige qu'un transfert ou une divulgation de données à caractère personnel à la suite d'une décision des tribunaux ou d'une autorité administrative d'un pays tiers ne puissent être reconnus ou exécutoires que s'ils se basent sur un accord international en vigueur conclu entre le pays tiers demandeur et l'Union ou un État membre, sans préjudice des autres motifs de transfert prévus par le chapitre V du RGPD. En effet, l'EDPB rappelle que «*une demande provenant d'une autorité étrangère ne constitue pas en soi un motif légal de transfert. Une telle requête ne peut être reconnue que "si elle se base sur un accord international, comme un traité d'assistance mutuelle, en vigueur conclu entre le pays*

[64] Voir WP 254 rev.01, p. 6.

[65] Voir WP 254 rev.01, p. 6.

[66] Voir l'article 44 du RGPD, notamment sa dernière phrase: «*Toutes les dispositions du présent chapitre sont appliquées de manière à ce que le niveau de protection des personnes physiques garanti par le présent règlement ne soit pas compromis*».

[67] Voir l'arrêt *Schrems I*, point 91.

*tiers demandeur et l'Union ou un État membre"*»[68]. Il est dès lors crucial que des dispositions substantiellement équivalentes puissent être relevées dans le droit britannique.

104. Dans le projet de décision, la Commission européenne rapporte certaines des explications fournies par les autorités britanniques selon lesquelles, en vertu de la *common law* ou de textes de loi, une décision de justice étrangère demandant des données n'est pas exécutoire au Royaume-Uni en l'absence d'accord international, et tout transfert de données à la demande d'une juridiction ou d'une autorité administrative étrangères nécessite un outil de transfert tel qu'un règlement d'adéquation ou des garanties appropriées, à moins que l'une des dérogations prévues à l'article 49 du RGPD britannique s'applique. Cependant, les échanges entre la Commission européenne et les autorités britanniques[69] à cet égard n'ont pas été communiqués à l'EDPB, qui n'est donc pas en mesure d'analyser et d'évaluer de manière indépendante si les garanties fournies par les autorités britanniques suffisent à assurer un niveau de protection substantiellement équivalent s'agissant des garanties prévues par l'article 48 du RGPD.

105. **L'EDPB invite la Commission européenne à fournir des garanties supplémentaires et des références spécifiques à la législation britannique qui garantissent que le niveau de protection assuré au titre du cadre juridique britannique est substantiellement équivalent à celui assuré au sein de l'EEE. Par conséquent, l'EDPB invite la Commission européenne à fournir des explications et des engagements écrits de la part des autorités britanniques en ce qui concerne la mise en œuvre de protections substantiellement équivalentes à celles prévues dans l'article 48 du RGPD.**

106. **L'EDPB estime qu'il est d'autant plus important de relever des dispositions du droit britannique assurant un niveau de protection substantiellement équivalent en lien avec les garanties prévues par l'article 48 à la lumière des inquiétudes précédemment exprimées concernant les demandes d'accès à des données au Royaume-Uni présentées par les autorités des États-Unis ou d'autres pays tiers, et compte tenu du fait que, en vertu de la décision d'adéquation, des données à caractère personnel pourraient être transférées depuis l'EEE vers le Royaume-Uni sans aucune garantie ni aucun engagement contraignant supplémentaires de la part du destinataire en ce qui concerne les demandes d'accès aux données soumises par les autorités d'autres pays tiers.**

## 3.2. Mécanismes en matière de procédure et d'application

107. Sur la base des critères de référence pour l'adéquation dans le cadre du RGPD, l'EDPB a analysé les aspects suivants du cadre du Royaume-Uni relatif à la protection des données, visés dans le projet de décision: l'existence et le fonctionnement efficace d'une autorité de contrôle indépendante; l'existence d'un système assurant un niveau de conformité satisfaisant, et un système d'accès à des mécanismes de recours appropriés donnant à toute personne dans l'Union les moyens d'exercer ses droits et d'obtenir réparation sans être confrontée à de lourds obstacles à l'exercice des voies de recours administratives et judiciaires.

### 3.2.1 Autorité de contrôle indépendante compétente

108. L'EDPB salue les efforts déployés par la Commission européenne pour examiner de manière exhaustive la création, le fonctionnement et les pouvoirs de l'autorité de contrôle britannique, au chapitre 2.6 du projet de décision. Au Royaume-Uni, le commissaire à l'information est responsable

[68] Voir l'annexe à la réponse conjointe de l'EDPB et du CEPD à la commission LIBE sur l'incidence de la loi CLOUD des États-Unis sur le cadre juridique européen régissant la protection des données à caractère personnel, adoptée le 10 juillet 2019, https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en.

[69] Voir note de bas de page 78 du projet de décision.

de la surveillance et de l'application de la conformité au RGPD britannique et à la DPA de 2018. Selon l'annexe 12 de la DPA de 2018, le commissaire à l'information est une «entité unipersonnelle», c'est-à-dire une entité juridique distincte constituée d'une seule personne, assistée d'un bureau, l'ICO.

109. En ce qui concerne l'indépendance du commissaire à l'information, l'EDPB souligne que l'article 51 du RGPD britannique ne précise pas expressément qu'il s'agit d'une autorité publique indépendante, comme le requiert l'article 51 du RGPD en ce qui concerne les autorités de contrôle. L'EDPB reconnaît néanmoins que le RGPD britannique reflète d'une manière similaire dans son article 52 les mêmes règles en matière d'indépendance que celles prévues à l'article 52, paragraphes 1 à 3, du RGPD.

110. En outre, l'EDPB souligne que l'article 52 du RGPD britannique ne prévoit pas d'obligations correspondant à celles de l'article 52, paragraphes 4 à 6, du RGPD, qui prévoient expressément que les autorités de contrôle concernées doivent disposer des ressources nécessaires à l'exécution effective de leurs missions et à l'exercice de leurs compétences. L'EDPB reconnaît cependant que la DPA de 2018 contient des dispositions ayant pour objectif d'assurer le financement approprié de l'ICO[70], et que l'ICO est à l'heure actuelle l'une des plus grandes autorités de contrôle comparée aux autorités de contrôle de l'Union/l'EEE. Puisqu'il est impératif d'allouer de manière constante des ressources appropriées, notamment en ce qui concerne le personnel et le budget[71], à une autorité de contrôle pour garantir son bon fonctionnement et lui permettre de s'acquitter de l'ensemble des missions qui lui sont confiées (ce que le Parlement européen a également reconnu comme un élément crucial[72]), l'EDPB estime qu'il est essentiel de porter une attention particulière aux évolutions futures dans ce domaine.

111. **Par conséquent, l'EDPB invite la Commission européenne à observer toute évolution concernant l'allocation de ressources à l'ICO qui pourrait nuire à la bonne exécution de ses missions.**

### 3.2.2. Existence d'un système de protection des données assurant un niveau de conformité satisfaisant

112. Le projet de décision réalise un examen complet des compétences que l'article 58 du RGPD britannique et la DPA de 2018 confèrent à l'ICO afin d'assurer le suivi et l'application de la législation. L'EDPB reconnaît que l'article 58 du RGPD britannique reflète de manière très similaire les mêmes règles en matière de compétences des autorités de contrôle que celles prévues à l'article 58 du RGPD. En ce qui concerne le pouvoir d'infliger des amendes administratives en fonction des circonstances propres à chaque cas, l'article 83 du RGPD britannique contient les mêmes dispositions et les mêmes montants maximaux que ceux prévus à l'article 83 du RGPD. Ainsi, l'EDPB considère que le cadre juridique britannique dans ce domaine est à l'heure actuelle conforme aux normes définies dans la législation pertinente de l'Union. À cet égard, l'EDPB souligne néanmoins que l'existence de sanctions *effectives* joue un rôle important s'agissant de garantir le respect des règles[73].

113. **Au vu de ce qui précède, l'EDPB invite la Commission européenne à surveiller le caractère effectif des sanctions et des voies de recours pertinentes dans le cadre du Royaume-Uni relatif à la protection des données.**

---

70 Voir les articles 137, 138 et 182 et l'annexe 12, paragraphe 9, de la DPA de 2018.

71 Voir WP 254 rev.01, p. 7.

72 Résolution du Parlement européen du 25 mars 2021 concernant le rapport d'évaluation de la Commission sur la mise en œuvre du règlement général sur la protection des données deux ans après son entrée en application, point 15, https://www.europarl.europa.eu/doceo/document/B-9-2021-0211_FR.html.

73 Voir WP 254 rev.01, p. 7.

#### 3.2.3. Le système de protection des données doit fournir un appui et aider les personnes concernées dans l'exercice de leurs droits et des mécanismes de recours appropriés

114. Un mécanisme de surveillance efficace, qui permet d'enquêter de manière indépendante sur les réclamations reçues afin de déterminer et de sanctionner les violations des droits des personnes concernées en pratique, ainsi que des voies de recours administratives et judiciaires efficaces (y compris une indemnisation en cas de dommages subis du fait du traitement illicite des données à caractère personnel des personnes concernées) sont des éléments essentiels à prendre en compte pour déterminer si un système de protection des données assure un niveau de protection adéquat.

115. L'EDPB salue le fait que l'ICO ait fourni des informations et des lignes directrices complètes sur son site internet, dans le but de renforcer la sensibilisation des responsables du traitement et des sous-traitants concernant leurs obligations et leurs devoirs, ainsi que d'aider les personnes concernées à s'informer sur leurs droits en matière de données à caractère personnel et à faire valoir leurs droits au titre du RGPD britannique et de la DPA de 2018.

116. **Nonobstant l'état actuel des choses, l'EDPB invite la Commission européenne à suivre de manière continue le niveau d'assistance que l'ICO apporte spécifiquement aux personnes dont les données à caractère personnel ont été transférées au Royaume-Uni en vertu de la décision d'adéquation, afin de les aider à exercer les droits que leur confère le régime britannique de protection des données.**

# 4. ACCÈS AUX DONNÉES À CARACTÈRE PERSONNEL TRANSFÉRÉES DE L'UNION EUROPÉENNE ET UTILISATION DE CELLES-CI PAR LES AUTORITÉS PUBLIQUES AU ROYAUME-UNI

## 4.1. Accès aux données et utilisation de celles-ci par les autorités publiques du Royaume-Uni à des fins répressives

### 4.1.1. Bases juridiques et limitations/garanties applicables

117. En ce qui concerne l'appréciation réalisée par la Commission européenne et rapportée aux considérants 132 et suivants du projet de décision en ce qui concerne **l'accès à des fins répressives**, la Commission européenne fournit des informations nuancées et détaillées et parvient en général à des conclusions compréhensibles. L'EDPB s'abstiendra donc de reproduire la plupart des constatations factuelles et des appréciations dans le présent avis. Cependant, dans certains cas, la description des faits ou l'explication des conclusions ne sont pas suffisantes pour que l'EDPB les embrasse.

#### 4.1.1.1. Utilisation du consentement

118. L'EDPB prend bonne note du fait que la Commission européenne affirme, dans la note de bas de page 184 du projet de décision[74], que l'**utilisation du consentement** n'est pertinente dans aucun des scénarios d'adéquation puisque dans les situations de transfert, les autorités répressives britanniques ne collectent pas directement les données auprès des personnes concernées sur la base de leur consentement. En conséquence, la Commission européenne n'évalue pas l'utilisation du consentement comme base juridique aux fins de l'exercice de pouvoirs de police.

[74] Voir la page 37 du projet de décision.

119. À cet égard, l'EDPB rappelle que l'article 45, paragraphe 2, point a), du RGPD imposer d'évaluer un vaste éventail d'éléments, ne se limitant pas aux situations de transfert, notamment «*l'état de droit, le respect des droits de l'homme et des libertés fondamentales, la législation pertinente, tant générale que sectorielle, y compris en ce qui concerne* […] *le droit pénal*».

120. L'EDPB observe, également sur la base des informations fournies par la Commission européenne au considérant 38 de son projet de décision d'exécution conformément à la directive (UE) 2016/680 du Parlement européen et du Conseil concernant le niveau de protection adéquat des données à caractère personnel au Royaume-Uni (ci-après le «projet de décision d'adéquation LED»), que l'utilisation du consentement, telle que prévue par le régime britannique dans un contexte répressif, devrait toujours reposer sur une base juridique. Cela signifie que même si la police dispose du pouvoir légal de traiter des données aux fins d'une enquête, dans certains cas spécifiques (par exemple pour procéder à la collecte d'un échantillon d'ADN), elle peut juger approprié de demander le consentement de la personne concernée.

121. **L'EDPB invite la Commission européenne à introduire dans la décision d'adéquation son analyse de l'utilisation possible du consentement dans un contexte répressif, prévue dans le projet de décision d'adéquation LED**.

#### 4.1.1.2. Mandats de perquisition et injonctions de production

122. Bien que l'EDPB n'ait aucun commentaire à formuler concernant l'obtention d'éléments de preuve par la police au moyen de mandats de perquisition et d'ordres de production d'éléments de preuve de manière générale, il découle du considérant 136 du projet de décision que la Commission européenne a articulé ses considérations en matière d'accès à des fins répressives autour de la police et qu'elle s'est moins penchée sur le traitement des données à caractère personnel par d'autres autorités répressives.

123. Par exemple, le cadre explicatif du Royaume-Uni pour la discussion relative à l'adéquation, section F: Contexte répressif[75], laisse entendre, à la p. 11, que la **National Crime Agency** (le service national britannique de lutte contre la criminalité, ci-après la «NCA») pourrait être une autorité répressive revêtant un intérêt particulier, assurant entre autres une fonction plus large de renseignement en matière pénale. La NCA décrit sa mission comme consistant à réunir des renseignements provenant d'un éventail de sources afin d'en optimiser l'analyse, l'évaluation et les opportunités tactiques, notamment ceux provenant des interceptions techniques de communications, des autorités répressives partenaires au Royaume-Uni et à l'étranger, et des services de sécurité et de renseignement[76]. La NCA est également l'un des principaux interlocuteurs des autorités répressives partenaires internationales, et elle joue un rôle essentiel dans l'échange de renseignements en matière pénale[77].

[75] Voir le cadre explicatif relatif aux discussions sur l'adéquation, gouvernement du Royaume-Uni, section F: Contexte répressif, 13 mars 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

[76] Voir le site Internet de la National Crime Agency, *Intelligence: enhancing the picture of serious organised crime affecting the UK*, https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/intelligence-enhancing-the-picture-of-serious-organised-crime-affecting-the-uk.

[77] Bien que tous les renseignements traités par la NCA ne soient pas des données à caractère personnel, une part considérable de ceux-ci peuvent représenter des données personnelles, et les activités décrites ici sont différentes des activités classiques de la police, de sorte qu'une évaluation de l'accès aux données à caractère

124. L'EDPB prend en outre bonne note du fait que le Government Communications Headquarters (service britannique du renseignement électronique, ci-après le «GCHQ»), dont les activités relèvent généralement de la partie 4 de la DPA de 2018, c'est-à-dire de la sécurité nationale, joue également un rôle actif s'agissant de réduire les préjudices sociaux et financiers causés par la criminalité grave et organisée au Royaume-Uni, en collaboration étroite avec le Home Office, la NCA, Her Majesty's Revenue and Customs (HMRC) et d'autres services de l'État[78]. Ses activités concernent la lutte contre les violences sexuelles infligées aux enfants, contre la fraude, contre d'autres types d'infractions économiques, y compris le blanchiment de capitaux, contre l'utilisation des technologies à des fins pénalement répréhensibles, contre la cybercriminalité; contre les infractions organisées en matière d'immigration, y compris la traite des êtres humains, et contre les drogues, les armes à feu et les autres types d'activité de contrebande.

125. **L'EDPB appelle la Commission européenne à compléter son analyse par une analyse des agences qui interviennent dans le domaine de l'application de la loi, qui semblent avoir fait de la collecte et de l'analyse des données, y compris des données à caractère personnel, un élément central de leurs activités quotidiennes, notamment de la NCA. De plus, l'EDPB invite la Commission européenne à s'intéresser de plus près aux agences comme le GCHQ, dont les activités relèvent à la fois de l'application de la loi et de la sécurité nationale, ainsi qu'au cadre juridique applicable à ces agences en ce qui concerne le traitement des données à caractère personnel.**

#### 4.1.1.3. Pouvoirs d'enquête à des fins répressives

126. Conformément au chapitre 4 des critères de référence pour l'adéquation dans le cadre du RGPD, intitulé «Garanties essentielles dans les pays tiers pour l'accès **à des fins répressives** et de sécurité nationale afin de limiter les interférences avec les droits fondamentaux», l'EDPB rappelle que «*[d]ans ce contexte, la Cour souligne également de manière critique que la précédente décision relative à la sphère de sécurité "ne comporte aucune constatation quant à l'existence, aux États-Unis, de règles à caractère étatique destinées à limiter les éventuelles ingérences dans les droits fondamentaux des personnes dont les données sont transférées depuis l'Union vers les États-Unis,* ***ingérences que des entités étatiques de ce pays seraient autorisées à pratiquer lorsqu'elles poursuivent des buts légitimes****, tels que la sécurité nationale"*»[79]. Dans ces critères de référence, l'EDPB affirme que les **quatre garanties**

personnel par les autorités répressives au Royaume-Uni serait incomplète en l'absence d'une évaluation complète des activités de la NCA. Il paraît raisonnable de s'assurer que les principes de protection des données revêtent le même sens pour toutes les agences des forces de l'ordre concernées et donc de faire toute la lumière sur les agences particulièrement axées sur les données, comme la NCA. De plus, dans la partie intitulée «looking for the future», l'explication se poursuit: «*nous cherchons en permanence de nouvelles possibilités de collecter, de faire évoluer et d'améliorer les capacités traditionnelles afin d'accroître la quantité et la qualité des renseignements disponibles pour être exploités, au Royaume-Uni comme à l'étranger*». «*Dans ce cadre, nous sommes en train de mettre au point une nouvelle capacité nationale d'exploitation des données, qui tire parti des pouvoirs que la loi portant création de la NCA (Crime and Courts Act) confère à notre agence afin de relier, de consulter et d'exploiter les données détenues par les différentes agences gouvernementales*». […] «*Cela nous permettra d'accroître notre souplesse et notre flexibilité s'agissant de répondre aux nouvelles menaces et d'agir de manière proactive, afin de collecter et d'analyser des informations et des renseignements concernant les menaces émergentes et de pouvoir agir avant que ces menaces ne se concrétisent*».

[78] Voir le site internet du GCHQ, Mission, Serious and Organised Crime, https://www.gchq.gov.uk/section/mission/serious-crime.

[79] Voir WP 254 rev.01, p, 9.

**européennes essentielles**[80] **doivent être respectées** pour que l'accès aux données, que ce soit à des fins de sécurité nationale ou à des fins d'application de la loi, **par tous les pays tiers soit considéré comme adéquat**, et notamment qu'**il convient de démontrer la nécessité et la proportionnalité au regard des objectifs légitimes poursuivis.**

127. La Commission européenne conclut cette section du projet de décision (considérant 139) en affirmant qu'«*[é]tant donné que ces pouvoirs d'enquêtes ciblés prévus par l'IPA de 2016 sont identiques à ceux des agences de sécurité nationale, les conditions, les limitations et les garanties applicables à ces pouvoirs sont détaillées à la section relative à l'accès aux données à caractère personnel et à l'utilisation de celles-ci par les autorités publiques du Royaume-Uni à des fins de sécurité nationale*». Toutefois, il ressort de la jurisprudence de la CJUE que, lorsqu'on applique le critère de la nécessité et de la proportionnalité à la législation des États membres autorisant la conservation des données à caractère personnel et l'accès à celles-ci par les autorités publiques, des objectifs légitimes tels que la sécurité nationale ou la lutte contre la criminalité grave sont des objectifs différents et, par conséquent, que l'un peut justifier un certain type d'ingérence sans que ce soit le cas de l'autre[81].

128. **L'EDPB souhaiterait donc disposer, dans la décision, d'une appréciation spécifique de la nécessité et de la proportionnalité des conditions, des limites et des garanties décrites dans les considérants 174 et suivants, qui constituent une section consacrée aux mesures visant des objectifs de sécurité nationale, en ce qui concerne leur application dans le contexte d'une mesure poursuivant un objectif d'application de la loi. Il invite donc la Commission européenne à davantage préciser si la conservation des données à caractère personnel et l'accès à celles-ci qu'elle décrit à des fins d'application de la loi sont suffisamment limités, de sorte à garantir un niveau de protection équivalent à celui assuré dans l'Union.**

#### 4.1.2. Utilisation ultérieure des informations collectées à des fins répressives (considérants 140-154)

129. L'EDPB note que le cadre du Royaume-Uni relatif à la protection des données prévoit des garanties et des limites équivalentes à celles établies par le droit de l'Union en lien avec l'utilisation ultérieure des informations collectées à des fins répressives.

##### 4.1.2.1. Utilisation ultérieure à d'autres fins répressives

130. La DPA de 2018 autorise en effet le traitement ultérieur des données collectées par une autorité compétente à des fins répressives (par le responsable initial du traitement ou par un autre responsable du traitement) pour toute autre finalité répressive, à condition que le responsable du traitement soit autorisé par la loi à traiter ces données pour une telle finalité et que le traitement soit nécessaire et proportionné à cette autre finalité. La Commission européenne fait observer que toutes les garanties prévues par la partie 3 de la DPA de 2018 s'appliquent au traitement effectué par l'autorité destinataire. L'EDPB souligne toutefois que, dans la partie 3 de la DPA de 2018, l'article 44, paragraphe 4, l'article 45, paragraphe 4, l'article 48, paragraphe 3 et l'article 68, paragraphe 7, prévoient la possibilité de limiter les droits des personnes concernées et l'article 79, la délivrance de certificats attestant qu'une restriction représente une mesure nécessaire et proportionnée afin de défendre la sécurité nationale. **L'EDPB recommande donc que la Commission**

[80] Voir les recommandations 02/2020 de l'EDPB sur les garanties essentielles européennes pour les mesures de surveillance.

[81] Voir l'arrêt de la CJUE dans les affaires jointes C-511/18, C-512/18 et C-520/18, La Quadrature du Net e.a., 6 octobre 2020, ECLI:C:2020:791.

**européenne évalue plus en détail l'éventuel impact de ces restrictions sur le niveau de protection dont bénéficient les données à caractère personnel en ce qui concerne l'utilisation ultérieure des informations collectées. De même, il y a également lieu de fournir des précisions supplémentaires concernant le cadre juridique britannique autorisant un tel partage ultérieur, notamment concernant la loi sur l'économie numérique (Digital Economy Act) de 2017 et la loi sur le droit pénal et la juridiction pénale (Crime and Courts Act) de 2013, qui permet le partage d'informations avec la NCA.**

#### 4.1.2.2. Utilisation ultérieure à des fins autres que les fins répressives au Royaume-Uni

131. La DPA de 2018 prévoit également que les données à caractère personnel collectées à l'une quelconque des fins répressives peuvent être traitées à des fins autres que répressives lorsque ce traitement est autorisé par la loi. Dans ce cas, l'article 19 de la loi sur la lutte contre le terrorisme (Counter-Terrorism Act) de 2008 constitue la base juridique autorisant ce partage. À ce sujet, l'EDPB fait observer que la Commission européenne n'a pas pleinement tenu compte de la portée et des dispositions de l'article 19 de la loi sur la lutte contre le terrorisme dans son évaluation et que cette disposition pourrait impliquer une utilisation d'une nature plus large, notamment eu égard au paragraphe 2 de cet article, qui prévoit que «*les informations obtenues par tout service de renseignement en ligne avec l'exercice de l'une de ses fonctions peuvent être utilisées par ce service en lien avec l'exercice de ses autres fonctions*».

132. L'EDPB note également que la Commission européenne pourrait davantage étayer, en indiquant notamment les actes législatifs de l'ordre juridique britannique qui établissent clairement et précisément de telles limites, son affirmation selon laquelle puisque les autorités compétentes sont des autorités publiques qui doivent agir conformément à la CEDH, notamment à son article 8, tout partage de données entre les agences répressives et les services de renseignement est conforme à la législation sur la protection des données et à la CEDH.

#### 4.1.2.3. Utilisation ultérieure dans le contexte des transferts ultérieurs en dehors du Royaume-Uni

133. Bien que la Commission européenne ait mentionné le fait que l'accord CLOUD Act est susceptible d'affecter les transferts ultérieurs à destination des États-Unis effectués par des FSCI se trouvant au Royaume-Uni, l'EDPB souligne également que l'entrée en vigueur de cet accord pourrait aussi affecter l'utilisation ultérieure des informations collectées par leur transfert ultérieur effectué par les autorités répressives au Royaume-Uni, notamment s'agissant de la délivrance et de la transmission d'ordres au titre de l'article 5 de cet accord.

134. De manière plus générale, l'EDPB estime que la conclusion d'accords bilatéraux futurs avec des pays tiers à des fins de coopération en matière répressive, qui fournit une base juridique au transfert de données à caractère personnel vers ces pays, pourrait également affecter les conditions d'utilisation ultérieure des informations collectées puisque de tels accords peuvent avoir une incidence sur le cadre du Royaume-Uni relatif à la protection des données tel qu'il a été évalué. L'EDPB recommande donc à la Commission européenne de soumettre ce point à une analyse supplémentaire en vérifiant l'existence d'accords internationaux, et de préciser si les dispositions de ces accords peuvent affecter l'application du droit britannique en matière de protection des données, ainsi que d'établir des limites ou des dérogations supplémentaires en lien avec l'utilisation ultérieure et la divulgation à l'étranger d'informations collectées à des fins répressives. L'EDPB estime que ces informations et cette appréciation sont essentielles afin de permettre la réalisation d'une évaluation complète du niveau de protection garanti par le cadre législatif et les pratiques britanniques en lien avec les divulgations et les utilisations ultérieures à l'étranger.

#### 4.1.3. Contrôle

135. L'EDPB fait observer que le contrôle des agences des forces de l'ordre est assuré par différents commissaires, en plus de l'ICO. Les décisions d'adéquation en projet mentionnent le commissaire aux pouvoirs d'enquête (IPC), le commissaire à la conservation et à l'utilisation de matériaux biométriques ainsi que le commissaire aux caméras de vidéosurveillance. Dans ce contexte, il convient de noter que la CJUE a souligné à de nombreuses reprises qu'un contrôle indépendant est nécessaire. L'IPC revêt une importance particulière concernant les questions d'accès aux données à caractère personnel transférées vers le Royaume-Uni. L'EDPB croit comprendre que l'IPC est un «commissaire judiciaire», à l'instar d'autres commissaires judiciaires, auquel il est possible de s'adresser dans le contexte du chapitre sur la sécurité nationale et que ces commissaires judiciaires bénéficient de la même indépendance que les juges, également dans le cadre de leur fonction de commissaire. En ce qui concerne le service de l'IPC, la Commission européenne explique au considérant 245 du projet de décision qu'il fonctionne de manière indépendante, en tant qu'«organisme indépendant», tout en étant financé par le Home Office.

136. L'EDPB n'a trouvé aucune indication supplémentaire dans le projet de décision visant à évaluer l'indépendance du commissaire à la conservation et à l'utilisation de matériaux biométriques ou du commissaire aux caméras de vidéosurveillance.

137. **La Commission européenne est invitée à évaluer plus en détail l'indépendance des commissaires judiciaires, également dans les cas où le commissaire n'agit pas (ou plus) en tant que juge, ainsi qu'à évaluer l'indépendance du commissaire à la conservation et à l'utilisation des matériaux biométriques et du commissaire aux caméras de vidéosurveillance.**

### 4.2. Cadre juridique général sur la protection des données dans le domaine de la sécurité nationale

#### 4.2.1. Certificats de sécurité nationale

138. Selon l'article 111 de la DPA de 2018, les responsables du traitement peuvent demander des certificats de sécurité nationale délivrés par un ministre, un membre du cabinet, le procureur général ou l'avocat général d'Écosse, attestant que les dérogations aux obligations et aux droits consacrés par les dispositions des parties 4 à 6 de la DPA de 2018 constituent des mesures nécessaires et proportionnées pour la protection de la sécurité nationale. Ces certificats ont vocation à assurer une plus grande sécurité juridique pour les responsables du traitement et ils constitueront une preuve concluante du fait que la sécurité nationale est applicable lors du traitement des données à caractère personnel. Il convient cependant de noter que ces certificats ne sont pas nécessaires pour se prévaloir de dérogations au titre de la sécurité nationale mais qu'ils constituent plutôt une mesure de transparence[82].

139. Lecture faite des articles 17 et 18 de l'annexe 20 de la DPA de 2018, l'EDPB pense comprendre que cette loi prolonge les effets d'un certificat de sécurité nationale délivré au titre de la loi de 1998 sur la protection des données (ci-après un «ancien certificat») aux fins du traitement des données à caractère personnel jusqu'au 25 mai 2019. Jusqu'à cette date, sauf s'ils avaient été remplacés ou

[82] Voir Home Office, The Data Protection Act 2018, National Security Certificates guidance, août 2020, paragraphe 4, p. 3, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.

révoqués, les anciens certificats étaient traités comme s'ils avaient été délivrés au titre de la DPA de 2018.

140. Cependant, lorsqu'un certificat de sécurité nationale délivré au titre de la loi de 1998 sur la protection des données n'indique aucune date d'expiration expresse, l'EDPB pense comprendre que ce certificat continuera de produire ses effets à l'égard du traitement en vertu de cette loi, sauf à être révoqué ou annulé[83]. Même si la protection assurée par ces anciens certificats se limite au traitement des données à caractère personnel au titre de la loi de 1998 sur la protection des données, l'EDPB prend acte du fait qu'il est possible de délivrer de nouveaux certificats de sécurité nationale au titre de cette loi pour les données à caractère personnel traitées en vertu de cette loi[84].

141. **Par souci d'exhaustivité, l'EDPB invite la Commission européenne à préciser dans son projet de décision que des certificats de sécurité nationale peuvent toujours être délivrés au titre de la loi de 1998 sur la protection des données. De plus, l'EDPB invite la Commission européenne à décrire dans son projet de décision les mécanismes de recours et de contrôle s'agissant des certificats délivrés au titre de la loi de 1998 sur la protection des données. Enfin, l'EDPB invite la Commission européenne à inclure dans son projet de décision le nombre de certificats existants délivrés au titre de la loi de 1998 sur la protection des données et à assurer un suivi attentif de cet aspect.**

#### 4.2.2. Droit de rectification et d'effacement

142. En ce qui concerne le droit de rectification et d'effacement, l'EDPB prend bonne note du fait que, conformément aux articles 100 et 149 de la DPA de 2018, les personnes concernées ont la possibilité de demander à la High Court [ou, en Écosse, à la Court of Session (juridiction supérieure écossaise en matière civile)] d'ordonner à un responsable du traitement de rectifier ou d'effacer leurs données dans les meilleurs délais.

143. **L'EDPB souligne que l'exercice des droits des personnes concernées doit être effectivement garanti: par conséquent, il invite la Commission européenne à décrire dans son projet de décision la manière dont l'article 100 de la DPA de 2018 fonctionne en pratique et à suivre de près l'application de cet article.**

#### 4.2.3. Exemptions pour des motifs de sécurité nationale

144. L'EDPB souhaite attirer l'attention sur l'article 110 de la DPA de 2018, et notamment sur l'annexe 11, qui définit les objectifs spécifiques aux fins desquels les services de renseignement peuvent s'affranchir de certains principes de protection des données, notamment en ce qui concerne les droits des personnes concernées, et ne sont pas tenus de signaler les violations des données à caractère personnel à l'ICO[85].

145. **L'EDPB demande à la Commission européenne de préciser davantage la portée des dérogations, car il s'interroge sur la pertinence pour le travail des services de**

[83] Voir Home Office, The Data Protection Act 2018, National Security Certificates guidance, août 2020, p. 5.
[84] Voir Home Office, The Data Protection Act 2018, National Security Certificates guidance, août 2020, paragraphe 8, p. 5.
[85] Ces objectifs sont la prévention et la détection de la «criminalité», les «informations que la loi oblige à divulguer, etc. ou liées à une procédure juridique», le «secret parlementaire», les «procédures en justice», les «honneurs et fonctions honorifiques accordés par la Couronne», les «forces armées», la «prospérité économique», la «confidentialité des professionnels du droit», les «négociations», les «références confidentielles fournies par le responsable du traitement», les «sujets et notes d'examens», les «recherches et les statistiques» et l'«archivage dans l'intérêt du public».

**renseignement de toutes les dérogations prévues à l'annexe 11 de la DPA de 2018, et se demande si elles assurent une équivalence avec les principes de nécessité et de proportionnalité.** Plus particulièrement, **l'EDPB invite la Commission européenne à apporter davantage de précisions sur les circonstances dans lesquelles un service de renseignement pourrait invoquer l'article 10 de l'annexe 11 de la DPA de 2018, qui affirme que «*[l]es dispositions énumérées ne s'appliquent pas aux données à caractère personnel qui consistent en une transcription des intentions du responsable du traitement en lien avec toute négociation menée avec la personne concernée dans la mesure où l'application des dispositions énumérées serait susceptible de nuire aux négociations*».**

### 4.3. Accès aux données et utilisation de celles-ci par les autorités publiques britanniques à des fins de sécurité nationale

146. De manière générale, l'EDPB reconnaît que les États disposent d'un large pouvoir d'appréciation en matière de sécurité nationale, ce que reconnaît également la CouEDH. L'EDPB rappelle également que, comme il le souligne dans ses recommandations mises à jour sur les garanties essentielles européennes pour les mesures de surveillance[86], l'article 6, paragraphe 3, du traité sur l'Union européenne dispose que les droits fondamentaux énoncés dans la CEDH constituent des principes généraux du droit de l'Union. Toutefois, comme le rappelle la CJUE dans sa jurisprudence, la CEDH ne constitue pas, tant que l'Union n'y a pas adhéré, un instrument juridique formellement incorporé dans l'ordre juridique de l'Union[87]. Dès lors, le niveau de protection des droits fondamentaux exigé par l'article 45 du RGPD doit être déterminé sur la base des dispositions dudit règlement, lues à la lumière des droits fondamentaux consacrés par la charte. Cela étant, conformément à l'article 52, paragraphe 3, de la charte, les droits contenus dans cette dernière et les droits correspondants garantis par la convention européenne des droits de l'homme doivent avoir la même signification et la même portée que ceux énoncés dans la CEDH: partant, comme l'a rappelé la CJUE, il convient de tenir compte de la jurisprudence de la CouEDH relative aux droits déjà prévus dans la charte des droits fondamentaux de l'Union européenne en tant que seuil de protection minimale en vue de l'interprétation des droits correspondants de la charte[88]. Toutefois, conformément à l'article 52, paragraphe 3, dernière phrase, de la charte, «*[c]ette disposition ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue*».

147. Par conséquent, dans l'évaluation qui suit, l'EDPB a tenu compte de la jurisprudence de la CouEDH, dans la mesure où la charte des droits fondamentaux de l'Union européenne, telle qu'interprétée par la CJUE, ne confère pas un niveau de protection plus élevé qui prescrirait des conditions différentes de celles de la jurisprudence de la CouEDH.

#### 4.3.1. Bases juridiques, limitations et garanties - pouvoirs d'enquête exercés dans le cadre de la sécurité nationale

##### 4.3.1.1. Observations générales

148. L'EDPB rappelle que l'IPA de 2016 est une loi récente qui a modifié plusieurs dispositions de la loi de 1994 sur les services de renseignement. Elle définit la mesure dans laquelle certains pouvoirs

[86] Voir les recommandations 02/2020 de l'EDPB sur les garanties essentielles européennes pour les mesures de surveillance.

[87] Voir l'arrêt *Schrems II*, point 98.

[88] Voir les affaires jointes de la CJUE, C-511/18, C-512/18 et C-520/18, *La Quadrature du Net e.a.*, ECLI:EU:C:2020:791, point 124.

d'enquête peuvent être exercés pour porter atteinte à la vie privée[89]. Malgré deux rapports de l'IPC qui fournissent des informations utiles concernant l'application de ce nouveau cadre juridique, aucun examen de certains aspects n'a encore été effectué, notamment en ce qui concerne les sélecteurs et les critères de recherche utilisés.

149. En outre, à titre de remarque générale concernant l'IPA de 2016 et son champ d'application, l'EDPB souligne les quatre points d'attention suivants:

150. En ce qui concerne le **premier point d'attention** relatif aux caractéristiques de la loi, l'EDPB souhaite relever deux éléments:

151. Premièrement, l'EDPB observe que la loi fait référence à des objectifs généraux pour l'utilisation des procédures prévues par l'IPA de 2016 et non à des catégories de personnes susceptibles d'être concernées par la collecte de données sur la base des parties 2 à 7 de l'IPA de 2016. À cet égard, l'EDPB rappelle qu'il doit exister un lien entre les catégories de personnes pouvant faire l'objet de mesures de surveillance et les objectifs poursuivis par la législation pour définir le champ d'application personnel de la loi.

152. Par ailleurs, l'EDPB souligne également que les définitions des termes «opérateurs de télécommunications», «service de télécommunications» et «système de télécommunications», qui déterminent le champ d'application de la loi, sont également très larges et, dans une certaine mesure, peu précises. En effet, l'EDPB relève que ces notions, dans le cadre de l'IPA de 2016, doivent être comprises de manière beaucoup plus large que dans le cadre des législations en matière de télécommunications, telles que définies par exemple dans le code des communications électroniques européen[90]. L'EDPB observe que les définitions de «service de télécommunication» et de «système de télécommunication» dans la loi sont censées être intentionnellement larges afin de rester pertinentes au regard des nouvelles technologies. De même, la définition d'un opérateur de télécommunications est également très large, et pourrait par exemple inclure les jeux vidéo en ligne avec une fonction de chat, ou d'autres sites Internet en ligne simplement parce qu'ils comprennent des fenêtres de chat[91].

153. En outre, si des procédures et un contrôle concernant l'évaluation de la nécessité et de la proportionnalité de la collecte et de l'accès aux données sont généralement prévus, les critères permettant de procéder à une telle évaluation ne sont pas définis dans la loi elle-même. Des indications supplémentaires peuvent être apportées par d'autres documents, tels que des codes de bonnes pratiques.

154. Toutefois, comme cela est rappelé dans les recommandations 02/2020 de l'EDPB sur les garanties essentielles européennes pour les mesures de surveillance, la CJUE a déclaré que «*l'exigence selon*

[89] Voir l'article 1er de l'IPA de 2016.

[90] Voir, par exemple, l'article 2, paragraphe 5 du code des communications électroniques européen qui définit le «service de communications interpersonnelles» comme «*un service normalement fourni contre rémunération qui permet l'échange interpersonnel et interactif direct d'informations via des réseaux de communications électroniques entre un nombre fini de personnes, par lequel les personnes qui amorcent la communication ou y participent en déterminent le ou les destinataires et qui ne comprend pas les services qui rendent possible une communication interpersonnelle et interactive uniquement en tant que fonction mineure accessoire intrinsèquement liée à un autre service*».

[91] Voir ministère de l'intérieur, code de bonnes pratiques relatif à l'interception des communications, mars 2018, paragraphes 2.5 et suivants, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

*laquelle toute limitation de l'exercice des droits fondamentaux doit être prévue par la loi implique que la base légale qui permet l'ingérence dans ces droits doit définir elle-même la portée de la limitation de l'exercice du droit concerné*»[92]. Plus précisément, la CJUE a expliqué que «*[p]our satisfaire à l'exigence de proportionnalité, une réglementation doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus*. *Cette réglementation doit être légalement contraignante en droit interne et, en particulier, indiquer en quelles circonstances et sous quelles conditions une mesure prévoyant le traitement de telles données peut être prise, garantissant ainsi que l'ingérence soit limitée au strict nécessaire*»[93].

155. La CouEDH a également souligné l'importance de la clarté de la loi «*pour indiquer à tous de manière adéquate en quelles circonstances et sous quelles conditions elle habilite la puissance publique à prendre pareilles mesures secrètes»*.[94]

156. **L'EDPB invite donc la Commission européenne à approfondir son évaluation concernant la précision, la clarté et l'exhaustivité de la loi concernée, et à fournir des éléments supplémentaires pour démontrer que celle-ci offre un niveau de protection substantiellement équivalent à celui garanti au sein de l'UE au regard des caractéristiques de la loi. L'EDPB souligne encore que les définitions larges devraient également être évaluées au regard de la proportionnalité des mesures d'interception.**

157. En outre, bien que divers codes internes des autorités compétentes de la communauté du renseignement développent partiellement certains de ces éléments, par exemple en ce qui concerne l'évaluation de la nécessité et de la proportionnalité de la collecte de données, l'EDPB souligne que les exigences de la CJUE relatives à la nature de la loi impliquent que les éléments essentiels, y compris la possibilité pour les individus de s'en prévaloir dans le cadre d'un recours, doivent être prévus dans la législation conférant des droits opposables[95]. En effet, l'article 6 de l'annexe 7 de l'PA de 2016 mentionne le fait que les tribunaux (et les autorités de surveillance) «*prennent en compte le fait qu'une personne n'a pas tenu compte d'un code pour statuer sur une question dans le cadre d'une telle procédure*» sans préciser si des personnes physiques peuvent invoquer une violation des codes devant les tribunaux (ou les autorités de surveillance). En outre, les éléments fournis jusqu'à présent dans le projet de décision se réfèrent soit à la reconnaissance par la CouEDH de la prévisibilité des règles énoncées[96] dans ces codes, plutôt qu'à la possibilité d'attaquer la décision

[92] Voir l'arrêt *Schrems II*, point 175; et la jurisprudence citée, ainsi que l'affaire C-623/17, *Privacy International/Secretary of State for Foreign and Commonwealth Affairs et autres*, 6 octobre 2020, ECLI:EU:C:2020:790 (ci-après «Privacy International»), point 65.

[93] Voir l'arrêt *Privacy International*, point 68.

[94] Voir arrêt de la CouEDH du 4 décembre 2015 dans l'affaire *Zakharov c. Russie*, EC:ECHR:2015:1204JUD004714306, point 229.

[95] À cet égard, la CJUE a considéré, par exemple, que la PPD-28 aux États-Unis ne remplissait pas les conditions requises, bien qu'elle prévoie également certaines limitations en ce qui concerne la collecte en vrac, voir *Schrems II*, point 181.

[96] Voir arrêt de la CouEDH du 13 septembre 2018 dans l'affaire *Big Brother Watch e.a./Royaume-Uni*, ECLI:CE:ECHR:2018:0913JUD005817013 (ci-après «Big Brother Watch»), point 325: «*Ce code étant un document public, soumis à l'approbation des deux chambres du Parlement, et dont doivent tenir compte les personnes qui exercent des missions d'interception ainsi que les tribunaux, la Cour a déjà expressément admis que ses dispositions pouvaient être prises en considération lors de l'examen de la prévisibilité du régime découlant de la RIPA*.»

devant les tribunaux, comme l'exige la CJUE, soit au fait que les tribunaux britanniques ont, dans certains cas, fait référence aux codes, alors qu'aucun des cas mentionnés n'illustre la possibilité pour des personnes d'agir en justice sur le fondement de droits dérivés des codes. **S'il est conclu que le droit britannique n'indique pas suffisamment les circonstances et les conditions dans lesquelles une mesure peut être adoptée et que ces éléments sont en fait fournis par les codes internes des autorités de la communauté du renseignement, l'EDPB demande à la Commission européenne d'approfondir son évaluation pour déterminer si les limitations et les garanties prévues dans les différents codes internes des autorités de la communauté du renseignement peuvent être invoquées par les personnes physiques devant un tribunal et être appliquées.**

158. Le **deuxième point d'attention** concerne le fait que les dispositions relatives, d'une part, à l'acquisition et à la conservation ciblées des données de communication et, d'autre part, à la collecte en masse, figurant dans l'IPA de 2016, ou dans d'autres législations telles que la loi de 1994 sur les services de renseignement, ou la loi de 2000 portant réglementation des pouvoirs d'enquête, s'appliqueront également aux données transférées de l'UE vers le Royaume-Uni. En ce qui concerne la collecte en masse, l'EDPB souligne que les dispositions pertinentes de la législation britannique autorisent la collecte de données en dehors du Royaume-Uni; cela pourrait donc inclure les données en transit transférées de l'EEE au Royaume-Uni sur la base de la décision d'adéquation[97]. De plus, l'EDPB remarque que la Commission européenne indique que «*[i]l convient de noter que généralement, la conservation et l'acquisition de données de communication ne concernent pas les données à caractère personnel de personnes concernées de l'Union européenne transférées vers le Royaume-Uni au titre de la présente décision. L'obligation de conserver ou de divulguer les données de communication au titre des parties 3 et 4 de l'IPA de 2016 concerne les données collectées par des opérateurs de télécommunications au Royaume-Uni directement auprès des utilisateurs d'un service de télécommunications*.»[98] Néanmoins, l'EDPB insiste sur le manque de clarté concernant le fait que seuls les établissements de ces opérateurs qui sont situés au Royaume-Uni peuvent recevoir des demandes de la part des autorités britanniques compétentes puisque la définition de l'opérateur de télécommunications figurant à l'article 261, paragraphe 10, de l'IPA de 2016 précise qu'«un opérateur de télécommunications est une personne qui offre ou fournit un service de télécommunications à des personnes au Royaume-Uni *ou qui contrôle ou fournit un système de télécommunications situé (entièrement ou partiellement) au Royaume-Uni ou contrôlé depuis le Royaume-Uni*». Par conséquent, les données à caractère personnel des personnes concernées dans l'EEE pourraient effectivement être visées, par exemple dans le cas de données collectées ou générées par un établissement d'un opérateur de télécommunications britannique situé dans l'EEE, transférées à un établissement de ce même opérateur situé au Royaume-Uni sur la base de la décision d'adéquation (à des fins commerciales), puis collectées, au Royaume-Uni, par les autorités publiques compétentes.

159. **L'EDPB estime donc que l'évaluation de ces dispositions est également pertinente pour l'évaluation du niveau d'adéquation du cadre juridique britannique et invite la Commission européenne à préciser cet aspect et à évaluer de manière approfondie dans quelle mesure c'est le cas. En particulier, l'EDPB demande à la Commission européenne de préciser sa conception du champ d'application de cette législation, notamment ce que recouvre la notion d'«utilisateurs de services de télécommunications», et si les données provenant d'établissements d'opérateurs de télécommunications situés en dehors du Royaume-Uni, dans la mesure où les données des**

[97] Voir les points 183 et suivants de l'arrêt *Schrems II* concernant l'évaluation d'une législation prévoyant l'accès à des données en transit entre l'UE et un pays tiers dans le cadre d'une décision d'adéquation.

[98] Voir considérant 196 du projet de décision.

**personnes concernées de l'EEE sont visées, pourraient faire l'objet d'une demande, étant donné la définition très générale des opérateurs de télécommunications.**

160. Le **troisième point d'attention** concerne la procédure de «double autorisation». L'EDPB constate qu'une nouvelle procédure de «double autorisation» a été introduite dans l'IPA de 2016. Néanmoins, l'EDPB comprend également que même si la collecte ou l'accès aux données à des fins de sécurité nationale ou de renseignement ne peut avoir lieu, en principe, que sur la base d'un mandat approuvé par un commissaire judiciaire, l'IPA de 2016 prévoit que «*dans des cas spécifiques et limités, l'interception légale sans mandat est possible et seule est requise l'autorisation préalable par les autorités compétentes de la commission à l'information [voir infra la section sur la surveillance], y compris en ce qui concerne les interceptions effectuées en réponse à des demandes étrangères (article 52 de l'IPA de 2016)*». Comme indiqué ci-après, cela correspond également aux préoccupations de l'EDPB en ce qui concerne, notamment, les divulgations à l'étranger. Par ailleurs, l'EDPB note que pour l'interférence avec le fonctionnement d'équipements, qu'il soit spécifique ou en masse, une dérogation à la procédure de double autorisation est également possible, et que le commissaire judiciaire est habilité à approuver uniquement le renouvellement des mandats de surveillance de masse, après une période initiale maximale de six mois. **L'EDPB demande à la Commission européenne d'approfondir son évaluation et de démontrer que, même dans les cas où la procédure de double autorisation ne s'applique pas, le cadre juridique britannique prévoit des garanties appropriées, y compris sous la forme d'un contrôle ex post efficace et grâce aux possibilités de recours ouvertes aux personnes physiques, afin de garantir que le niveau de protection assuré est substantiellement équivalent à celui offert au sein de l'UE (voir également infra section 4.3.3 sur le contrôle).**

161. Par ailleurs, bien que l'IPA de 2016 ait effectivement introduit la procédure de «double-lock» (double autorisation), l'EDPB reste préoccupé par certaines caractéristiques de la nouvelle législation. Suite à la présentation des sections correspondantes du projet de décision, l'EDPB a analysé les types de collecte et d'accès aux données suivants dans le même ordre que celui présenté par la Commission européenne. L'ordre des éléments évalués ci-après ne reflète donc pas une hiérarchie relative au niveau de préoccupation de l'EDPB.

#### 4.3.1.2. Acquisition et conservation ciblées de données de communication

162. L'EDPB relève que deux fonctionnaires peuvent accorder des autorisations ciblées pour l'obtention de données de communication: l'ordonnateur du Bureau des autorisations relatives à la communication de données (ci-après «l'IPC»), un haut fonctionnaire désigné (une personne occupant une fonction ou un rang prescrit au sein d'une autorité publique compétente), auxquels s'ajoute l'approbation par un commissaire judiciaire dans certains cas. Cependant, il est difficile pour l'EDPB de déterminer exactement, en vertu de la loi et du code pertinent, quel fonctionnaire autorise quel type d'acquisition ciblée de données de communication, et dans quelle mesure un fonctionnaire désigné serait suffisamment indépendant[99].

163. **L'EDPB demande donc à la Commission européenne d'approfondir l'évaluation de cet aspect et de fournir des explications plus précises sur ces éléments.**

164. Concernant la notification demandant la conservation des données de communication, l'EDPB note également que de tels avis peuvent être adressés à une «description des opérateurs». Cette notion semble signifier qu'il est possible de demander à plusieurs opérateurs en même temps de conserver

[99] Voir également infra concernant l'évaluation de la procédure de double autorisation et l'indépendance du commissaire judiciaire.

toutes les données. En effet, la nature ciblée de l'acquisition ne concerne pas le nombre des opérateurs, mais le nom ou la description des personnes, des organisations, du lieu ou du groupe de personnes qui constituent la «cible», une description de la nature de l'enquête et une description des activités pour lesquelles l'équipement est utilisé. L'EDPB souligne donc que, selon le nombre d'opérateurs concernés par cette «description des opérateurs», la notification peut être plus étendue que ce que la procédure de conservation ciblée semble impliquer. **L'EDPB invite la Commission européenne à approfondir l'évaluation de cet aspect, et à fournir des assurances supplémentaires que, même lorsque les avis sont adressés à plusieurs opérateurs, ils restent limités à ce qui est strictement nécessaire et proportionné.**

#### 4.3.1.3. Interférence dans le fonctionnement des équipements

165. L'EDPB note que «l'interférence dans le fonctionnement des équipements» peut déroger à la procédure de double autorisation en cas d'urgence[100]. L'EDPB est dès lors préoccupé par le fait que les objectifs pouvant justifier qu'une telle interférence dans le fonctionnement des équipements soit requise sont larges, et que les critères d'urgence restent flous (en cas d'urgence, une autorisation ex ante par le commissaire judiciaire, après une évaluation de la nécessité et de la proportionnalité de l'interférence avec des équipements, n'est pas requise). Étant donné que dans cette dernière situation, «le mandat cesse de produire ses effets et ne peut être renouvelé» lorsque le commissaire judiciaire n'approuve pas ex post l'interférence avec le fonctionnement d'équipements, l'EDPB comprend que les données collectées dans l'intervalle restent légalement collectées. Pour que ces données soient effacées, une ordonnance spécifique du commissaire judiciaire peut être émise[101].

166. **L'EDPB demande à la Commission européenne d'approfondir l'évaluation des conditions dans lesquelles l'urgence peut être invoquée, et de fournir des précisions concernant les voies d'exercice des droits possibles pour les personnes concernées, et les voies de recours possibles qui leur sont ouvertes dans le contexte d'opérations d'exploitation de réseaux informatiques, en particulier lorsqu'elles ont lieu dans un contexte d'urgence conduisant à une dérogation à la procédure de double autorisation.**

#### 4.3.1.4. Interception massive de données à partir des canaux de transmission

167. Comme décrit dans le rapport sur l'examen des pouvoirs de surveillance de masse[102], «*l'interception massive implique généralement la collecte de communications alors qu'elles transitent par des canaux de transmission particuliers (liaisons de communication).*» La fiche d'information officielle de la loi IPA de 2016 décrit l'«interception massive*» comme «le processus de collecte d'un volume de communications suivi de la sélection de communications spécifiques à lire, regarder ou écouter lorsque cela est nécessaire et proportionné.*» L'EDPB observe que l'«interception massive» de données implique en réalité la collecte de données avant même tout filtrage par des sélecteurs (soit simple dans le cadre de la surveillance d'individus dont on sait déjà qu'ils représentent une menace, soit complexe, dans le cadre de l'identification de nouvelles menaces et de personnes d'intérêt jusque-là inconnues).

168. L'acquisition de données de communication en masse était également l'une des questions examinées par la CJUE dans l'affaire Privacy International, qui a donné lieu à un arrêt de la grande

[100] Voir l'article 109 de l''IPA de 2016.
[101] Voir l'article 110, paragraphe 3, point b), de l'IPA de 2016.
[102] Voir le rapport sur l'examen des pouvoirs de surveillance de masse, par le contrôleur indépendant de la législation sur le terrorisme, août 2016.

chambre rendu le 6 octobre 2020 (outre la question de savoir si cette collecte de données relevait du champ d'application du droit de l'UE, même à des fins de sécurité nationale). L'IPA de 2016 a remplacé la législation qui faisait l'objet de cet arrêt.

169. L'EDPB observe qu'avec l'introduction de l'IPA de 2016 dans le droit britannique, un mandat est désormais également nécessaire pour intercepter des données en masse. Le processus de délivrance de ce mandat repose sur la détermination des «objectifs opérationnels». La liste de ces objectifs opérationnels est établie par les chefs des services de renseignement, puis approuvée par le Secrétaire d'État. Cette décision est elle-même approuvée par un commissaire judiciaire indépendant qui doit vérifier si le mandat est nécessaire et proportionné aux objectifs opérationnels. L'EDPB comprend que le commissaire judiciaire est habilité à évaluer non pas les objectifs opérationnels eux-mêmes, mais si le mandat est nécessaire et proportionné aux objectifs opérationnels énumérés dans le mandat. La commission du parlement britannique chargée du contrôle des services de renseignement reçoit une copie de la liste tous les trois mois, et le Premier ministre examine la liste de ces objectifs opérationnels au moins une fois par an.

170. Cependant, sur la base des éléments fournis par la Commission européenne dans le projet de décision, il semble difficile d'évaluer la portée des objectifs opérationnels mentionnés dans la liste et de déterminer si la collecte des données qu'ils permettent atteint le seuil fixé par la CJUE (par exemple, la limitation de la collecte de données à une zone géographique pourrait être limitée à quelques rues, ou à la collecte de données provenant de l'EEE dans son ensemble).

171. En outre, l'EDPB souligne que les données collectées en masse peuvent être conservées pendant de longues périodes (afin d'être disponibles pour un accès ultérieur à des fins d'examen). De fait, l'EDPB rappelle que l'article 150, paragraphes 5 et 6, de l'IPA de 2016 ne prévoit que la destruction des copies de données collectées, et ce uniquement si leur conservation n'est pas nécessaire, ou n'est pas susceptible de le devenir, dans l'intérêt de la sécurité nationale ou de tout autre motif entrant dans le champ d'application de l'article 138, paragraphe 2, de l'IPA de 2016, ou si leur conservation n'est pas nécessaire dans le cadre de plusieurs autres objectifs[103]. L'EDPB souligne que ces motifs semblent très généraux et qu'en tout état de cause, seules des copies des données obtenues sont mentionnées.

172. Par ailleurs, l'EDPB observe que dans les cas urgents, l'IPA de 2016 permet également de modifier les mandats sans l'approbation préalable d'un commissaire judiciaire, et que dans ce cas, si le commissaire judiciaire consulté ex post, dans les trois jours ouvrables suivant la modification, refuse d'approuver la modification, le mandat produit ses effets comme si la modification n'avait pas été effectuée, mais les données collectées entre-temps restent collectées légalement[104]. Pour que ces données soient effacées, une ordonnance spécifique du commissaire judiciaire peut être émise[105].

173. **L'EDPB demande donc à la Commission européenne de nouvelles précisions sur les interceptions en masse et leur évaluation approfondie, en particulier concernant la sélection et le recours aux sélecteurs dans le cadre de ces procédures d'interception en masse, afin de préciser dans quelle mesure l'accès aux données à caractère personnel atteint le seuil fixé par la CJUE (voir également ci-dessous la section 4.3.1.7., en particulier sur la surveillance des sélecteurs), et quelles garanties existent pour protéger les droits fondamentaux des personnes dont les données sont interceptées dans ce contexte, notamment en ce qui concerne les durées de conservation des données. Une**

[103] Voir article 150, paragraphes 3 et 6, de l'IPA de 2016.
[104] Voir l'article 147 de l'IPA de 2016 (Partie 6, chapitre I).
[105] Voir l'article 181, paragraphe 3, point b), de l'IPA de 2016.

**évaluation indépendante des autorités de surveillance compétentes du Royaume-Uni serait particulièrement utile.**

174. **L'EDPB souligne également qu'il semble d'autant plus critique que les «communications liées à l'étranger» qui entrent dans le champ d'application des pratiques d'interception massive semblent impliquer que des données pourraient être directement interceptées et collectées en masse au sein de l'EEE par le Royaume-Uni, y compris les données en transit entre l'EEE et le Royaume-Uni qui entreraient dans le champ d'application du projet de décision (voir ci-dessous la section 4.3.2. sur l'utilisation ultérieure des informations collectées à des fins de sécurité nationale et de divulgation à l'étranger).**

#### 4.3.1.5. Protection et garanties pour les données secondaires

175. L'EDPB est également préoccupé par le fait que la législation britannique pertinente relative à l'interception de masse ne prévoit pas le même niveau de protection pour toutes les données de communication. Les «données secondaires», qui peuvent être obtenues avec un mandat d'interception massive, sont, selon l'article 137 de l'IPA de 2016, à la fois les «données relatives aux systèmes», «*qui sont comprises dans la communication, en font partie, y sont jointes ou y sont logiquement associées (par l'expéditeur ou autrement)*», et les «données d'identification», «*qui sont comprises dans la communication, en font partie, y sont jointes ou y sont logiquement associées (par l'expéditeur ou autrement), qui peuvent être logiquement séparées du reste de la communication et qui, lorsqu'elles sont ainsi séparées, ne révèlent rien de ce qui pourrait raisonnablement être considéré comme la signification (le cas échéant) de la communication, abstraction faite de toute signification découlant du fait de la communication ou de toute donnée relative à la transmission de la communication*»[106].

176. L'EDPB note que ces «données secondaires», également appelées «métadonnées»[107], collectées en masse, ne semblent pas bénéficier des mêmes garanties que les données collectées avec un mandat ciblé, ou que les données de contenu collectées en masse. En effet, l'EDPB remarque que la sélection de tout contenu intercepté bénéficie de plus de garanties[108] que la sélection de données secondaires[109].

[106] Les «données relatives aux systèmes» et les «données d'identification» sont définies à l'article 263 de l'IPA de 2016.
[107] Voir le rapport sur l'examen des pouvoirs de surveillance de masse, par le contrôleur indépendant de la législation sur le terrorisme, août 2016.
[108] Voir l'article 152, paragraphe 1, point c), et paragraphe 3 et suivant de l'IPA de 2016.
[108] Voir l'article 152, paragraphe 1, point c), et paragraphe 3 et suivant de l'IPA de 2016.
[109] Voir l'article 152, paragraphe 1, points a) et b), de l'IPA de 2016.

177. De plus, l'EDPB souligne que tant la CouEDH[110] que la CJUE[111] ont émis des doutes quant au fait que ces données soient moins sensibles que d'autres, et en particulier que les données de contenu. En effet, le code de bonnes pratiques concernant les interceptions présente comme exemples de «données secondaires» à la fois des «données système» telles que les configurations de routeurs, les adresses électroniques ou les identifiants d'utilisateurs, et également d'autres identifiants de compte, mais aussi des «données d'identification», telles que le lieu d'une réunion dans un rendez-vous de calendrier, des informations sur une photographie, telles que l'heure, la date et le lieu où elle a été prise. **L'EDPB souligne donc l'évaluation cohérente par la CouEDH et la CJUE, et rappelle les préoccupations exprimées à l'égard des données secondaires qui devraient bénéficier de garanties spécifiques en raison de leur sensibilité. En conséquence, l'EDPB invite la Commission européenne à évaluer de manière approfondie si les garanties prévues par la législation britannique pour cette catégorie de données personnelles assurent un niveau de protection substantiellement équivalent à celui qui est garanti dans l'UE.**

#### 4.3.1.6. Traitement automatisé des données de communication

178. L'EDPB constate que les autorités de la communauté du renseignement ne se contentent pas d'utiliser des sélecteurs simples ou complexes pour filtrer les données acquises en masse, mais qu'elles peuvent également s'appuyer sur d'autres outils de traitement automatisé pour analyser «*des volumes importants d'informations, ce qui permet aux agences de trouver également des liens, des modèles, des associations ou des comportements susceptibles de démontrer une menace grave nécessitant une enquête*», selon le rapport de la commission du parlement britannique chargée du contrôle des services de renseignement[112]. **L'EDPB est conscient du fait que ce rapport public concerne des pratiques relevant du cadre juridique précédent, qui a ensuite été remplacé par l'IPA de 2016.** Il estime néanmoins qu'une évaluation et un contrôle supplémentaires indépendants de l'utilisation d'outils de traitement automatisé par les autorités britanniques de contrôle compétentes sont nécessaires, et invite la Commission européenne à évaluer

[110] Voir arrêt de la CouEDH dans l'affaire *Big Brother Watch*, point 357, ayant fait l'objet d'un renvoi devant la grande chambre: «*En conséquence, même si la Cour ne doute pas que les données de communication associées constituent un outil essentiel pour les services de renseignement aux fins de leur activité de lutte contre le terrorisme et les infractions graves, elle considère qu'en les excluant intégralement des garanties applicables à l'analyse et à l'examen des données de contenu, les autorités n'ont pas ménagé un juste équilibre entre les intérêts publics et privés concurrents. Il ne s'agit pas de dire que les données de communication associées ne doivent être accessibles qu'aux fins de déterminer si un individu se trouve ou non dans les îles Britanniques, car cela reviendrait à exiger l'application de normes plus strictes aux données de communication associées qu'aux données de contenu, mais il faut que des garanties suffisantes assurent que les données de communication associées ne soient exclues des exigences posées à l'article 16 de la RIPA que dans la limite de ce qui est nécessaire pour déterminer si un individu se trouve actuellement dans les îles Britanniques.*»

[111] Voir l'arrêt de la CJEU, *Privacy International*, point 71: «*L'ingérence que comporte la transmission des données relatives au trafic et des données de localisation aux services de sécurité et de renseignement dans le droit consacré à l'article 7 de la charte doit être considérée comme étant particulièrement grave, compte tenu notamment du caractère sensible des informations que peuvent fournir ces données et, notamment, de la possibilité d'établir à partir de celles-ci le profil des personnes concernées, une telle information étant tout aussi sensible que le contenu même des communications. En outre, elle est susceptible de générer dans l'esprit des personnes concernées le sentiment que leur vie privée fait l'objet d'une surveillance constante (voir, par analogie, arrêts du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, points 27 et 37, ainsi que du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, points 99 et 100).*»

[112] Voir le rapport de la commission du parlement britannique chargée du contrôle des services de renseignement, «Privacy and Security: A modern and transparent legal framework», 2015, point xviii, p. 13, https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf.

plus en profondeur cette question ainsi que les garanties qui seraient et/ou pourraient être accordées aux personnes concernées de l'EEE dans ce contexte.

#### 4.3.1.7. Risques de conformité et pratiques non conformes des autorités compétentes de la communauté du renseignement

179. L'EDPB constate que des rapports de surveillance détaillés sont disponibles. Ils fournissent des éléments précieux concernant ce qu'ils jugent être des pratiques positives en matière de conformité, mais aussi sur les risques de conformité et les pratiques non conformes identifiés.

180. À cet égard, l'IPC indique dans son rapport pour 2019 que plusieurs éléments concernant l'application du cadre juridique par les diverses autorités compétentes ont révélé des (risques de) non-conformités de la part des autorités compétentes.

181. Tout d'abord, l'EDPB a observé que les critères permettant de classer un ensemble de données comme ensemble de données personnelles de masse ou comme données ciblées ne semblent pas toujours clairs pour le MI5 et le SIS eux-mêmes, en particulier pour le MI5, ce qui peut déboucher sur l'absence de garanties appropriées appliquées aux données[113]. Dans son rapport de 2019, l'IPC a suggéré que «*cette question devrait être résolue en priorité*»[114]. Toujours en ce qui concerne les ensembles de données personnelles en masse, l'EDPB note que pour le GCHQ, même si la classification des ensembles de données personnelles en masse semble être satisfaisante (bien qu'elle doive encore être vérifiée par l'IPC), l'examen de conformité interne des mandats par l'équipe spécialisée a suscité de sérieuses préoccupations en mars 2019, 50 % des justifications des mandats d'acquisition en masse examinés par l'équipe de conformité du GCHQ ne répondant pas à la norme requise. Selon l'IPC, l'équipe de conformité avait commencé à travailler pour enquêter sur ce problème et à former à nouveau le personnel pour améliorer cette norme. La formation actualisée sur les dispositions de la loi IPA de 2016 et la formation supplémentaire dispensée par les réseaux de politiques et de conformité (ci-après «PCN») ont permis d'améliorer la conformité du GCHQ dans ce domaine. L'IPC ne s'attend pas à constater un dérapage de cette norme lors des prochaines inspections, mais continuera à surveiller ce point de près[115]. **L'EDPB partage donc le point de vue selon lequel un examen et un contrôle supplémentaires desdits éléments par la Commission européenne sont nécessaires dans le cadre de l'évaluation du niveau de protection, afin de garantir l'amélioration de cette norme, comme le souligne le rapport de l'IPC, et rappelle que la mise en œuvre et l'application concrète du cadre**

[113] Voir le rapport annuel de 2019 du commissaire aux pouvoirs d'enquête, 15 décembre 2020, paragraphe 8.39, https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019_Web-Accessible-version_final.pdf: «*Nous avons observé le développement positif du [Bulk Oversight Panel (BOP) - Comité de surveillance des opérations visant le recueil de données en masse] et notons son impact dans la gestion de la conformité interne. Nous continuons à souhaiter plus de clarté concernant le processus utilisé par le MI5 pour effectuer des examens initiaux de nouveaux ensembles de données afin de mieux comprendre les décisions de classer un ensemble de données comme EDP ou, par exemple, comme données ciblées. Nous avons été préoccupés par une action non résolue dans le procès-verbal du BOP concernant la résolution des divergences entre les allocations d'EDP entre le MI5 et le SIS. Il est possible, en raison des différentes utilisations des données et des différentes combinaisons de données détenues, que les deux agences détiennent le même ensemble de données, ou des versions de celui-ci, et qu'elles puissent légalement être classées comme données de masse par l'une et comme données ciblées par l'autre. Il existe un risque que, si l'une des agences a à tort qualifié des données détenues de ciblées, ces données soient détenues sans mandat approprié et ne soient pas protégées par des garanties appropriées*.»

[114] Voir le rapport annuel de 2019 du commissaire aux pouvoirs d'enquête, paragraphe 8.39.

[115] Voir le rapport annuel de 2019 du commissaire aux pouvoirs d'enquête, paragraphe 10.48.

**juridique doivent également être prises en compte lors de l'évaluation de l'équivalence substantielle d'un pays tiers, comme le prévoit l'article 45 du RGPD.**

182. Plus généralement, l'EDPB souligne les points d'attention partagés par l'IPC concernant les «recherches basées sur les tâches» menées par les agents du MI5 - qui permettent à un enquêteur d'effectuer plus d'une recherche dans les ensembles de données personnelles en masse à sa disposition, et les «*risques sérieux de conformité associés à certains environnements technologiques utilisés par le MI5*», concernant la localisation des données stockées dans l'environnement, qui y a accès, dans quelle mesure elles sont copiées ou partagées, les processus de suppression qui leur sont appliqués, ainsi que les durées de conservation. Bien que l'IPC indique que des mesures ont été prises et que des garanties ont été introduites, certaines d'entre elles restent manuelles et gérées sur une base individuelle et humaine; cela montre qu'il est essentiel que le «*MI5 continue à maintenir ces nouveaux processus et à fournir des ressources suffisantes pour qu'ils fonctionnent efficacement. Si le MI5 identifie une augmentation des comportements non conformes*»[116]. L'IPC souhaite qu'ils soient portés à son attention dès que possible. **L'EDPB demande donc à la Commission européenne de contrôler étroitement ces aspects à l'avenir.**

183. En ce qui concerne le GCHQ, l'EDPB comprend également à la lecture du rapport de l'IPC que, pour les opérations menées dans le cadre des mandats de masse, «*la qualité des demandes d'approbation interne était variable et nous avons observé que la manière dont ces demandes étaient présentées pouvait être améliorée*»[117], et que pour les interférences ciblées avec des équipements, les explications concernant l'utilisation de descripteurs généraux étaient parfois trop générales et imprécises[118]. L'EDPB a également constaté que, dans le contexte de l'interférence massive dans le fonctionnement des équipements, l'IPC recommande que «*les applications devraient systématiquement et explicitement enregistrer le lien entre la cible, un objectif statutaire et les exigences en matière de renseignement*»[119], que «*toutes les applications devraient clairement prendre en compte le potentiel d'intrusion collatérale et les mesures d'atténuation pertinentes lors de l'évaluation de la proportionnalité*»[120], et souligne que, malgré les progrès accomplis, «*des améliorations sont encore possibles*»[121] et qu'une attention supplémentaire sera également nécessaire à l'avenir.

184. En ce qui concerne le régime d'interception en masse prévu par loi de 2000 portant réglementation des pouvoirs d'enquête (Regulation of Investigatory Powers Act 2000, ci-après «RIPA 2000»), qui a depuis été remplacé par les dispositions de la l'IPA de 2016, l'EDPB rappelle que la surveillance insuffisante, tant de la sélection des canaux de transmission d'Internet pour l'interception que du filtrage, de la recherche et de la sélection des communications interceptées pour examen, était, dans l'affaire *Big Brother Watch* renvoyée devant la grande chambre, l'un des aspects essentiels jugés incompatibles par la CouEDH avec l'article 8 de la CEDH s'agissant de la législation précédente relative aux pouvoirs d'investigation des autorités britanniques dans le contexte de la sécurité nationale. **L'EDPB invite la Commission européenne à vérifier l'état d'avancement de la procédure, à prendre en compte ces éléments et à les préciser dans la décision d'adéquation si celle-ci est adoptée par la Commission européenne.**

[116] Voir le rapport annuel de 2019 du commissaire aux pouvoirs d'enquête, paragraphe 8.52.
[117] Voir le rapport annuel de 2019 du commissaire aux pouvoirs d'enquête, paragraphe 10.2.
[118] Voir le rapport annuel de 2019 du commissaire aux pouvoirs d'enquête, paragraphes 10.16 et 10.17.
[119] Voir le rapport annuel de 2019 du commissaire aux pouvoirs d'enquête, paragraphe 10.23.
[120] Voir le rapport annuel de 2019 du commissaire aux pouvoirs d'enquête, paragraphe 10.23.
[121] Voir le rapport annuel de 2019 du commissaire aux pouvoirs d'enquête, paragraphe 10.23.

185. Dans cette affaire, la CouEDH: «*n'est pas persuadée que les garanties applicables à la sélection des canaux de transmission aux fins de l'interception de données et de leur sélection pour examen soient suffisamment solides pour constituer des garde-fous adéquats contre les abus. Cependant, l'élément le plus préoccupant est l'absence de supervision indépendante solide des sélecteurs et des critères de recherche utilisés pour filtrer les communications interceptées*.»[122] Comme l'a relevé l'IPC, «*cette constatation a fait écho à une recommandation similaire formulée par la commission du parlement britannique chargée du contrôle des services de renseignement dans son rapport de 2015 "Privacy and Security: A modern and transparent legal framework"*»[123]. **L'EDPB se félicite du fait que l'IPC a procédé par la suite à un examen de son approche de l'inspection de l'interception en masse en 2019, «*qui comprenait un examen minutieux des modalités techniquement complexes de la mise en œuvre effective de l'interception en masse*»[124] et s'est engagé à inclure «*un examen détaillé des sélecteurs et des critères de recherche auxquels la CouEDH a fait allusion ci-dessus*»[125] dans les inspections de l'interception en masse à partir de 2020. Compte tenu de l'importance de cet aspect, l'EDPB est préoccupé par le fait qu'un examen détaillé des sélectionneurs et des critères de recherche n'a pas encore été effectué par l'IPC, et appelle la Commission européenne à contrôler étroitement les développements à cet égard, d'autant plus que le format concret de ces contrôles reste à préciser[126].**

#### 4.3.2. Utilisation ultérieure des informations recueillies à des fins de sécurité nationale et de divulgation à l'étranger

186. S'agissant de l'utilisation ultérieure des informations collectées à des fins de sécurité nationale, la Commission européenne renvoie dans son évaluation à l'article 87, paragraphe 1 de la DPA de 2018, qui prévoit en effet que «*les données à caractère personnel ainsi collectées ne doivent pas être traitées d'une manière incompatible avec la finalité pour laquelle elles sont collectées*». L'EDPB précise toutefois que cette disposition peut faire l'objet d'exceptions liées à la sécurité nationale, conformément à l'article 110 de la loi de 2018. L'EDPB note par ailleurs que la législation prévoit la possibilité d'une «divulgation à l'étranger» pour l'interception et l'examen ciblés, mais aussi pour l'acquisition et la conservation ciblées de données de communication, pour l'interférence ciblée dans le fonctionnement d'équipements ou pour l'interception en masse et l'interférence massive dans le fonctionnement des équipements.

##### 4.3.2.1. Utilisation ultérieure, divulgation à l'étranger et cadre juridique applicable au Royaume-Uni

187. La Commission européenne a estimé que la partie 4 de la DPA de 2018, et en particulier son article 109, constituait une disposition pertinente définissant des exigences spécifiques pour l'utilisation ultérieure des informations collectées, et notamment pour le transfert international de données à caractère personnel par les services de renseignement vers des pays tiers ou des organisations internationales. Toutefois, l'EDPB note que l'article 110 de la loi de 2018 sur la protection des données prévoit une exception relative à la sécurité nationale précisant que certaines dispositions de ladite loi ne s'appliquent pas lorsqu'une telle exception est nécessaire pour la sauvegarde de la sécurité nationale. Les dispositions concernées qui peuvent ne pas s'appliquer comprennent le chapitre 2 de la partie 4 de la DPA de 2018 relatif aux principes de protection des

[122] Voir arrêt de la CouEDH dans l'affaire *Big Brother Watch*, point 347.
[123] Voir le rapport annuel de 2019 du commissaire aux pouvoirs d'enquête, paragraphe 10.28.
[124] Voir le rapport annuel de 2019 du commissaire aux pouvoirs d'enquête, paragraphe 10.28.
[125] Voir le rapport annuel de 2019 du commissaire aux pouvoirs d'enquête, paragraphe 10.28.
[126] Voir le rapport annuel de 2019 du commissaire aux pouvoirs d'enquête, paragraphe 10.28: «le format exact de cette inspection reste à convenir».

données, y compris la limitation de la finalité, ainsi que le chapitre 3 de la partie 4 de la loi relatif aux droits des personnes concernées. L'article 109 de la loi de 2018 sur la protection des données, lu conjointement avec l'article 110 et les conditions dans lesquelles celui-ci s'applique peuvent conduire à des cas où un transfert international de données à caractère personnel est effectué par les services de renseignement vers des pays tiers sans que soient appliquées les dispositions relatives aux principes de protection des données et aux droits des personnes concernées.

188. Comme l'a indiqué la Commission européenne, une telle exception doit être évaluée au cas par cas et ne peut être invoquée que dans la mesure où l'application d'une disposition particulière aurait des conséquences négatives pour la sécurité nationale. En effet, la délivrance d'un certificat national pour les services de renseignement britanniques vise à certifier qu'une exception est requise à l'égard de données personnelles déterminées qui sont traitées dans le but de sauvegarder la sécurité nationale. L'EDPB note toutefois que dans ses orientations relatives au certificat de sécurité nationale en vertu de la DPA de 2018, le ministère de l'Intérieur britannique précise que «[*i]l est important de noter dans un premier temps qu'un certificat n'est pas nécessaire pour invoquer l'exception de sécurité nationale; en fait, dans la plupart des cas, les contrôleurs détermineront eux-mêmes si l'exception de sécurité nationale est applicable*.» [127] En outre, la directive du ministère de l'Intérieur britannique précise que «*les certificats de sécurité nationale peuvent s'appliquer à des données à caractère personnel qui peuvent être spécifiquement identifiées ou couvrir une catégorie plus large de données à caractère personnel. Ils peuvent être aussi bien préventifs que rétrospectifs*.» [128] Une exception de sécurité nationale peut donc s'appliquer à un transfert international de données personnelles par les services de renseignement vers des pays tiers en l'absence d'un certificat de sécurité nationale.

189. De plus, l'EDPB relève que, par exemple, selon le certificat de sécurité nationale DPA/S27/Security Service[129], jusqu'au 24 juillet 2024, les données à caractère personnel traitées «*pour, au nom, à la demande ou avec l'aide ou l'assistance du Security Service ou*» et «*lorsque ce traitement est nécessaire pour faciliter le bon exercice des fonctions du Security Service décrites à l'article 1er de la loi de 1989 sur le service de sécurité*» sont exemptées des dispositions de la loi britannique correspondant au chapitre V du RGPD en ce qui concerne les transferts de données à caractère personnel vers des pays tiers ou des organisations internationales. Si les autres certificats de sécurité nationale accessibles au public ne prévoient pas une exception aux dispositions de l'article 109 de la DPA de 2018, il convient de rappeler que tout ou partie du texte d'un certificat de sécurité nationale peut être suspendu si sa publication est contraire aux intérêts de la sécurité nationale, à l'intérêt public ou susceptible de compromettre la sécurité de toute personne.

190. De manière générale, tout en évaluant le projet de décision au sujet de ces dispositions, l'EDPB observe que les garanties dont ces divulgations sont assorties comprennent uniquement l'exigence que le destinataire des données respecte les exigences en matière de sécurité des données, l'étendue de la divulgation limitée à ce qui est nécessaire, la conservation des données et la restriction de l'accès aux données à un nombre limité de personnes. Ainsi, **l'EDPB souligne que concernant des divulgations à l'étranger, l'application de l'exception de sécurité nationale prévue**

[127] Voir Ministère de l'Intérieur, The Data Protection Act 2018, directive relative aux certificats de sécurité nationale, août 2020, paragraphe 3, p. 3.
[128] Voir Ministère de l'Intérieur, The Data Protection Act 2018, directive relative aux certificats de sécurité nationale, août 2020, paragraphe 5, p. 4.
[129] Voir le certificat du secrétaire d'État, DPA/S27/Security Service, fondé sur l'article 27 de la loi sur la protection des données 2018, du 24 juillet 2019, https://ico.org.uk/media/about-the-ico/documents/nscs/2615660/nsc-part-2-mi5-201908.pdf.

**par la loi britannique peut conduire à des situations où les garanties assurant que les principes de limitation de la finalité, de nécessité et de proportionnalité, ainsi que les droits des individus, le contrôle et le recours ne seraient pas entièrement assurés ou respectés dans le pays tiers de destination. L'EDPB recommande ainsi à la Commission européenne de poursuivre son examen des garanties globales prévues dans le droit britannique concernant la divulgation outre-mer, notamment au regard de l'application des exceptions de la sécurité nationale.**

#### 4.3.2.2. Divulgation à l'étranger et partage de renseignements dans le cadre de la coopération internationale

191. L'EDPB note également que la Commission européenne n'a pas examiné, dans le cadre de son évaluation de l'adéquation, les accords internationaux existants conclus entre le Royaume-Uni et des pays tiers ou des organisations internationales susceptibles de prévoir des dispositions spécifiques concernant le transfert international de données à caractère personnel par les services de renseignement vers des pays tiers.

192. L'EDPB rappelle également que l'évaluation de la Commission européenne repose principalement sur l'évaluation de la partie 4 de la DPA de 2018, et se penche notamment sur le fait que l'IPA de 2016 se concentre sur les «demandes» d'échange de renseignements avec des partenaires étrangers, mais ne traite pas d'autres formes de partage de renseignements. L'EDPB note à cet égard que le projet de décision de la Commission européenne ne fait pas référence ou n'évalue pas l'articulation entre le cadre législatif britannique et le «UK-US Communication Intelligence Agreement» (accord Royaume-Uni - États-Unis en matière de renseignement relatif aux communications). Dans une déclaration récente marquant le 75e anniversaire de cet accord, l'Agence nationale de sécurité américaine (ci-après «NSA») a mentionné que ce partenariat permet «*de partager des informations entre les deux agences autant que possible, avec un minimum de restrictions»* et que *«ce document novateur a permis de créer les politiques et procédures pour les professionnels du renseignement britanniques et américains en matière de partage de communications, de traductions, d'analyses et d'informations de décryptage*.»[130] Cet accord est également devenu le fondement d'autres partenariats en matière de renseignement avec l'Australie, le Canada et la Nouvelle-Zélande.

193. La nature secrète de cet accord et ses dispositions spécifiques soulèvent un problème majeur quant à la clarté et la prévisibilité de la loi quant à l'utilisation ultérieure et à la divulgation à l'étranger d'informations collectées par les autorités britanniques à des fins de sécurité nationale. Dans ce contexte, l'EDPB rappelle qu'en ce qui concerne le niveau de protection garanti au sein de l'UE, la CJUE a souligné que la législation impliquant une ingérence dans le droit fondamental à la protection des données à caractère personnel doit «*prévoir des règles claires et précises régissant la portée et l'application d'une mesure et imposant un minimum d'exigences, de sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement leurs données contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données. La nécessité de disposer de telles garanties est d'autant plus importante lorsque les données à caractère personnel sont soumises à un traitement automatique et qu'il existe un risque important d'accès illicite à ces données*»[131]. Par conséquent, l'EDPB considère que la Commission européenne devrait prendre en compte l'impact de l'accord entre le Royaume-

[130] Voir le communiqué de presse de la NSA: «GCHQ and NSA Celebrate 75 Years of Partnership», 5 février 2021, https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2494453/gchq-and-nsa-celebrate-75-years-of-partnership/.
[131] Voir l'arrêt *Schrems I,* point 91.

Uni et les États-Unis en matière de renseignement relatif aux communications dans le cadre de son évaluation de l'adéquation.

194. La CouEDH, dans la première partie de l'arrêt qu'elle a rendu le 13 septembre 2018 dans l'affaire *Big Brother Watch*, a évalué le régime britannique de partage des renseignements et en particulier l'accord Royaume-Uni - États-Unis en matière de renseignement relatif aux communications. De fait, la CouEDH a déclaré que «*[c]e n'est pas la RIPA qui fixe le cadre légal en vertu duquel les services de renseignement britanniques peuvent demander à des services de renseignement étrangers des éléments interceptés. L'accord en matière de renseignement relatif aux communications... du 5 mars 1946 permet expressément l'échange d'éléments interceptés entre les États-Unis et le Royaume-Uni.*»[132] et a considéré qu'il existe «*une base légale à la demande de renseignements à des services de renseignement étrangers, et que la loi est suffisamment accessible*.»[133] Bien que la CouEDH ait conclu qu'il n'y a pas eu violation de l'article 8[134] de la CEDH en ce qui concerne le régime de partage des renseignements, l'EDPB constate que ce jugement a maintenant été renvoyé devant la grande chambre, dont la décision est toujours en attente. L'EDPB note également que, dans une opinion en partie concordante et en partie dissidente de cet arrêt, le juge Koskelo, rejoint par le juge Turković[135], a conclu à une violation de l'article 8 de la CEDH en ce qui concerne le régime de partage des renseignements, en déclarant qu'«*[i]l est facile de souscrire au principe selon lequel aucune modalité prévoyant l'obtention auprès de services de renseignement étrangers de renseignements provenant de communications interceptées – que la demande faite aux services étrangers soit de procéder à une telle interception ou d'en communiquer les résultats – ne devrait permettre de contourner les garanties qui doivent s'appliquer à toute surveillance menée par les autorités internes (paragraphes 216, 423 et 447). Toute autre approche serait d'ailleurs improbable*».

195. Comme l'ont montré plusieurs rapports des médias et d'organisations non gouvernementales[136][137], la version la plus récente de l'accord entre le Royaume-Uni et les États-Unis en matière de renseignements relatifs aux communications, qui a été rendue publique, date de 1956 et, depuis lors, les technologies de communication et la nature du renseignement d'origine électromagnétique ont considérablement évolué. Les médias ont par exemple révélé que les données transitant par des câbles sous-marins qui aboutissent au Royaume-Uni sont interceptées par le GCHQ et rendues accessibles à la NSA[138].

196. Pour l'EDPB, une question clé en matière de partage de renseignements est de savoir si l'article 109 de la DPA de 2018 et les dispositions de l'IPA de 2016 restent applicables lorsque les services de renseignement britanniques agissent conformément à l'accord entre le Royaume-Uni et les États-Unis en matière de renseignement relatifs aux communications. Un autre élément clé à évaluer est de savoir si les dispositions ou l'application effective de cet accord ont un impact sur le niveau de

[132] Voir arrêt de la CouEDH dans l'affaire *Big Brother Watch*, point 425.
[133] Voir arrêt de la CouEDH dans l'affaire *Big Brother Watch*, point 427.
[134] Voir arrêt de la CouEDH dans l'affaire *Big Brother Watch*, point 448.
[135] Voir arrêt de la CouEDH dans l'affaire *Big Brother Watch*, avis en partie concordant et en partie divergent du juge Koskelo, rejoint par le juge Turković.
[136] Voir BBC, «Diary reveals birth of secret UK-US spy pact that grew into Five Eyes», 5 mars 2021, https://www.bbc.com/news/uk-56284453.
[137] Voir «Privacy International, Policy Briefing - UK Intelligence Sharing Arrangements», avril 2018, https://privacyinternational.org/sites/default/files/2018-04/Privacy%20International%20Briefing%20-%20Intelligence%20Sharing%20%28UK%29%20FINAL.pdf.
[138] Voir The Guardian, Le GCHQ exploite les câbles en fibres optiques pour accéder secrètement aux communications mondiales., 21 juin 2013, https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

protection des données à caractère personnel en transit de l'EEE vers le Royaume-Uni, ou permettent un accès et une acquisition directs de données à caractère personnel par les services de renseignement d'autres pays tiers.

197. Par conséquent, outre les réserves exprimées à l'égard des «divulgations à l'étranger» sur la base de la partie 4 de la DPA de 2018 et de l'exception de sécurité nationale correspondante, ainsi que des demandes dans le cadre de l'IPA de 2016, **l'EDPB est préoccupé par d'autres formes de partage et de divulgation d'informations, sur la base d'autres instruments, en particulier les divers accords internationaux conclus par le Royaume-Uni avec d'autres pays tiers, plus particulièrement lorsque ces instruments restent inaccessibles au public, comme l'accord entre le Royaume-Uni et les États-Unis en matière de renseignements relatifs aux communications. L'incidence d'un tel accord pourrait entraîner un contournement des garanties liées à l'accès aux données à caractère personnel et à leur utilisation à des fins de sécurité nationale.**

198. En effet, l'EDPB partage le point de vue exprimé par le rapporteur spécial des Nations unies, Joe Cannatacci, selon lequel «*[l]e partage de renseignements ne doit pas constituer une porte dérobée permettant d'obtenir ou de faciliter pour d'autres l'obtention de renseignements échappant aux garanties nationales, ni une brèche permettant à des gouvernements étrangers ayant des normes inférieures en matière de protection de la vie privée (ou d'autres droits de l'homme) d'obtenir des renseignements auprès des services de renseignement britanniques qui pourraient donner lieu à des violations des droits de l'homme*»[139].

199. De plus, **l'EDPB considère que la conclusion d'accords bilatéraux ou multilatéraux avec des pays tiers aux fins de la coopération en matière de renseignement, fournissant une base juridique pour l'interception et l'acquisition directes de données à caractère personnel ou pour le transfert de données à caractère personnel vers ces pays, peut également affecter de manière significative les conditions d'utilisation ultérieure des informations collectées, étant donné que ces accords sont susceptibles d'affecter le cadre juridique britannique en matière de protection des données tel qu'évalué.**

### 4.3.3. Contrôle

200. L'EDPB souligne l'importance d'une supervision globale par des autorités de surveillance indépendantes pour un niveau adéquat de protection des données. La garantie d'indépendance des autorités de contrôle au sens de l'article 8, paragraphe 3, de la charte des droits fondamentaux de l'Union européenne vise à assurer un contrôle efficace et fiable du respect des règles de protection des personnes à l'égard du traitement des données à caractère personnel.

201. Lorsque des données à caractère personnel sont consultées et utilisées à des fins de sécurité nationale, la fonction de contrôle est principalement remplie par l'IPC et les commissaires judiciaires (ci-après les «commissaires judiciaires»).

202. **L'EDPB reconnaît que, de manière générale, l'introduction des commissaires judiciaires dans l'IPA de 2016 constitue une amélioration notable.** Conformément à une demande formulée plus haut, la Commission européenne est invitée à évaluer plus en détail l'indépendance des **commissaires judiciaires, et en particulier à déterminer dans quelle mesure l'indépendance de l'IPC et du Bureau**

[139] Voir la déclaration de fin de mission du rapporteur spécial sur le droit à la vie privée à l'issue de sa mission au Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, 29 juin 2018, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E#:~:text=Intelligence%20sharing%20must%20not%20result,UK%20intelligence%20that%20could%20give.

**du commissaire aux pouvoirs d'enquête (ci-après l'«IPCO») est légalement garantie, car ce point ne figure pas dans l'IPA de 2016.** Ceci est d'autant plus important que l'IPC statue sur les appels formés par le gouvernement, dans le cas où une demande de **mesure** de surveillance a été rejetée **par** un commissaire judiciaire.

203. L'IPC remplit des fonctions de surveillance ex ante et ex post. En ce qui concerne la surveillance ex ante, l'EDPB comprend que la fonction des commissaires judiciaires est d'approuver, dans des cas individuels, diverses mesures de surveillance, y compris l'interception ciblée et l'acquisition en masse de données de communication. L'EDPB observe également que la jurisprudence de la CJUE ne permet pas de déduire que l'approbation préalable des mesures de surveillance est une condition absolue de la proportionnalité des mesures de surveillance.[140]

204. Afin d'évaluer l'efficacité de ce niveau de surveillance, l'EDPB voit néanmoins la nécessité de préciser davantage les scénarios dans lesquels une interception légale sans approbation préalable des commissaires judiciaires est possible.

205. Dans son projet de décision, la Commission européenne mentionne dans les notes de bas de page 201 et 266 des «cas limités spécifiques» prévus par l'IPA de 2016 dans ses articles 44 à 52 en ce qui concerne les interceptions ciblées. L'EDPB observe que les articles 45 à 51 de l'IPA de 2016 sont des dérogations dont il est affirmé qu'elles ne sont pas régulièrement utilisées par les services de renseignement. Par ailleurs, l'EDPB **comprend** que dans les **cas où ces dérogations s'appliquent** (par exemple, les fournisseurs de télécommunications et de services postaux), l'approbation préalable par les commissaires judiciaires doit être délivrée dans le cas où les autorités répressives ou les services de renseignement **demandent** l'accès à ces données; **l'EDPB invite la Commission européenne à confirmer dans sa décision que cela est bien le cas.**

206. L'EDPB reconnaît que l'article 44, paragraphe 2, de l'IPA de 2016 permet l'interception de communications si l'une des parties (expéditeur ou destinataire) a donné son consentement et s'il existe une autorisation en vertu de la RIPA 2000 ou de la loi écossaise de 2000 portant réglementation des pouvoirs d'enquête (2000, loi du Parlement écossais 11), c'est-à-dire la situation juridique antérieure à la mise en place des commissaires judiciaires. L'EDPB **invite** la Commission européenne à préciser si cela signifie que, dans les cas où un consentement unilatéral a été donné, la procédure d'approbation préalable ne s'appliquerait pas du tout.

207. En ce qui concerne la surveillance ex post, il est également important de vérifier qu'une surveillance indépendante efficace est assurée sans faille, en particulier lorsqu'elle n'est pas prévue ex ante.

208. L'EDPB note que pour les articles 48 à 52 de l'IPA de 2016, un examen ex post par les commissaires judiciaires est effectué, et **invite la Commission européenne à préciser dans quelles conditions et à l'initiative de qui un tel examen** ex post **doit être effectué.**

209. Selon l'article 229, paragraphe 4, de l'IPA de 2016, l'IPC n'est pas tenu de contrôler l'exercice de certaines fonctions. À cet égard, l'EDPB invite la Commission européenne à clarifier les dispositions de l'article 229, paragraphe 4, points d) et e), de l'IPA de 2016 au regard de son impact pratique sur la compétence de contrôle de l'IPC. **L'EDPB tient pour acquis que le commissaire à l'information est l'autorité de surveillance compétente lorsque les dérogations prévues à l'article 229,**

[140] Cependant, elle note également que la CJUE, lorsqu'elle a invalidé le bouclier de protection des données dans l'affaire *Schrems II*, a pris note du fait que, en vertu du droit américain, la Cour dite FISC «*n'autorise pas de mesures de surveillance individuelles, mais plutôt des programmes de surveillance (comme PRISM ou UPSTREAM) sur la base de certifications annuelles*.» (point 179).

**paragraphe 4, de l'IPA de 2016 s'appliquent, et l'EDPB invite la Commission européenne à confirmer dans sa décision que cela est bien le cas.**

210. **Il apparaît que,** dans le cadre d'une surveillance ex post, le rôle de l'**IPC** se **limite** à formuler des recommandations en cas de non-conformité, et à avertir la personne concernée, si l'erreur est grave et qu'il est dans l'intérêt public que la personne soit informée. **L'EDPB invite la Commission européenne à clarifier comment l'IPCO peut effectivement assurer le respect de la loi.**

211. **Enfin, l'EDPB constate que les personnes concernées ne peuvent pas s'adresser directement à l'IPCO, mais doivent introduire une réclamation auprès de l'ICO qui, toutefois, a des compétences limitées dans le domaine de la sécurité nationale. L'EDPB invite donc la Commission européenne à clarifier davantage de quelle manière il est légalement garanti que l'IPCO traite les réclamations dans ces cas.**

#### 4.3.4. Voies de recours

212. À la lumière des arrêts *Schrems I* et *Schrems II* de la CJUE, il est clair qu'une protection juridictionnelle effective au sens de l'article 47 de la charte des droits fondamentaux de l'Union européenne revêt une importance fondamentale pour présumer de l'adéquation de la législation d'un pays tiers. Les arrêts ont également montré qu'une attention particulière, à cet égard, doit être accordée à la protection judiciaire effective dans le domaine de l'accès pour raison de sécurité nationale aux données personnelles.

213. **L'EDPB reconnaît que le Royaume-Uni a mis en place l'IPT. L'IPT est compétent pour connaître des affaires relatives à l'utilisation des pouvoirs d'enquête non seulement par les autorités répressives mais également par les services de renseignement. De ce que l'EDPB comprend, l'IPT fonctionne comme un tribunal au sens de l'article 47 de la charte des droits fondamentaux de l'UE. Quant à ses pouvoirs, la Commission européenne est invitée à confirmer que l'IPT dispose de tous les pouvoirs mentionnés au considérant 262 du projet de décision, quelle que soit la base juridique de la réclamation introduite.**

214. La surveillance discrète exercée par les agences de renseignement signifie souvent que l'objet de la surveillance, la personne concernée, n'a pas, et n'aura pas connaissance de la surveillance. Dans ce contexte, lorsqu'il a dû analyser le droit américain, l'EDPB a maintes fois exprimé son inquiétude quant à l'exigence de «qualité pour agir», telle qu'interprétée dans le droit américain, dans des affaires de surveillance. Dans ce contexte, l'EDPB note que la réclamation introduite devant l'IPT ne requiert qu'un test de «croyance», selon lequel l'auteur de la réclamation doit démontrer qu'il ou elle risque potentiellement de faire l'objet d'une mesure.

215. Dans son analyse de l'IPT, l'EDPB accorde également une attention particulière au fait que le fonctionnement de l'IPT a été à plusieurs reprises jugé conforme à la CEDH, telle qu'interprétée par la CouEDH.