Avis 15/2021 concernant le projet de décision d'exécution de la Commission européenne, rendu conformément à la directive (UE) 2016/680, constatant le niveau de protection adéquat des données à caractère personnel assuré par le Royaume-Uni

Adopté le 13 avril 2021

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Historique des versions

Version 1.1	6 juillet 2021	Changement de présentation
Version 1.0	13 avril 2021	Adoption de l'avis

TABLE DES MATIÈRES

Le comité européen de la protection des données,

vu l'article 51, paragraphe 1, point g), de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil[1] [ci-après la «directive (UE) 2016/680»],

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 assuré par le Royaume-Uni en vertu de la directive (UE) 2016/680 le 19 février 2021[2]. Elle 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 le «CEPD» ou le «comité»)[3]. L'évaluation par le CEPD du caractère adéquat du niveau de protection assuré par le 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. Dans le cadre de ces travaux, le comité s'est principalement référé à ses critères de référence pour l'adéquation dans le cadre de la directive en matière de protection des données dans le domaine répressif (ci-après les «critères de référence»[4], adoptés le 2 février 2021, ainsi qu'à la jurisprudence pertinente reflétée dans ses recommandations 02/2020 sur les garanties essentielles européennes pour les mesures de surveillance[5].

4. L'objectif principal du CEPD est de rendre à la Commission européenne un avis sur le caractère adéquat du niveau de protection accordé aux personnes physiques au Royaume-Uni. Il importe de reconnaître que le CEPD ne s'attend pas à ce que le cadre juridique britannique reproduise la législation européenne en matière de protection des données.

[1] JO L 119 du 4.5.2016, p. 89.
[2] Voir le communiqué de presse de la Commission européenne, communiqué de presse, Protection des données: la Commission européenne engage un processus concernant les flux de données à caractère personnel vers le Royaume-Uni, 19 février 2021: https://ec.europa.eu/commission/presscorner/detail/fr/ip_21_661.
[3] Idem.
[4] Voir les recommandations 01/2021 du CEPD sur les critères de référence pour l'adéquation dans le cadre de la directive en matière de protection des données dans le domaine répressif, adoptées le 2 février 2021: https://edpb.europa.eu/system/files/2021-05/recommendations012021onart.36led.pdf_fr.pdf.
[5] Voir les recommandations 02/2020 du CEPD sur les garanties essentielles européennes pour les mesures de surveillance, adoptées le 10 novembre 2020: https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_fr.pdf.

5. Le comité rappelle toutefois que, pour que la législation du pays tiers soit considérée comme assurant un niveau de protection adéquat, l'article 36 de la directive (UE) 2016/680 et la jurisprudence de la Cour de justice de l'Union européenne (ci-après la «CJUE») exigent qu'elle soit alignée sur l'essence des principes fondamentaux consacrés par la directive (UE) 2016/680. En ce qui concerne la protection des données, le CEPD constate qu'il existe une forte convergence entre le cadre de la directive (UE) 2016/680 et le cadre juridique britannique sur certaines dispositions essentielles, telles que, par exemple, les concepts (par exemple, «données à caractère personnel»; «traitement des données à caractère personnel;» «responsable du traitement»); 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 prise de décision automatisée et le profilage.

6. Le CEPD recommande à la Commission européenne de compléter son analyse par des informations sur l'existence d'un mécanisme permettant d'informer les autorités compétentes des États membres concernés de tout traitement ou divulgation ultérieurs par les autorités britanniques auxquelles ils ont transféré les données à caractère personnel, et d'en déterminer l'effectivité dans l'ordre juridique britannique.

7. Le CEPD estime que les dispositions du chapitre 5 de la partie 3 de la loi de 2018 sur la protection des données (Data Protection Act) prévoient, en principe, un niveau de protection substantiellement équivalent à celui garanti par le droit de l'Union en ce qui concerne le transfert de données à caractère personnel par une autorité répressive du Royaume-Uni vers un pays tiers.

8. Le CEPD constate la capacité du Royaume-Uni, en vertu de son cadre juridique, de reconnaître des territoires comme offrant un niveau adéquat de protection des données au regard du cadre britannique en matière de protection des données, mais souligne toutefois que cela pourrait entraîner des risques pour la protection des données à caractère personnel transférées depuis l'Union européenne, en particulier si, à l'avenir, le cadre de protection des données du Royaume-Uni s'écarte de l'acquis de l'Union. **Dès lors, dans les situations susmentionnées, la Commission européenne doit jouer son rôle de surveillance et, si le niveau de protection substantiellement équivalent des données à caractère personnel transférées depuis l'Union européenne n'est pas maintenu, elle doit envisager de modifier la décision d'adéquation afin d'introduire des garanties spécifiques pour les données transférées depuis l'Union, et/ou suspendre la décision d'adéquation.**

9. **Enfin, en ce qui concerne les accords internationaux conclus entre le Royaume-Uni et des pays tiers,** la Commission européenne est invitée à examiner l'interaction entre le cadre britannique en matière de protection des données et les engagements internationaux du Royaume-Uni, afin notamment de garantir la continuité du niveau de protection lorsque des données à caractère personnel sont transférées de l'Union européenne vers le Royaume-Uni sur la base de la décision d'adéquation du Royaume-Uni, puis transférées ultérieurement vers d'autres pays tiers; ainsi qu'à exercer un contrôle permanent et à prendre des mesures, le cas échéant, dans le cas où la conclusion d'accords internationaux entre le Royaume-Uni et des pays tiers risquerait de compromettre le niveau de protection des données à caractère personnel prévu dans l'Union européenne.

10. À cet égard, le CEPD attire l'attention sur le fait que l'entrée en vigueur de l'accord sur l'accès aux données électroniques à des fins de lutte contre la grande criminalité conclu entre le Royaume-Uni et les États-Unis d'Amérique (ci-après l'«accord Royaume-Uni/États-Unis sur la loi CLOUD»)[6] pourrait

[6] Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering

avoir une incidence sur les transferts ultérieurs par les autorités répressives britanniques, en ce qui concerne en particulier l'émission et la transmission d'ordres en vertu de l'article 5 de l'accord Royaume-Uni/États-Unis sur la loi CLOUD.

11. Le CEPD recommande également à la Commission européenne de contrôler en permanence si les futurs accords conclus avec des pays tiers aux fins de la coopération en matière répressive, qui fournissent une base juridique pour le transfert de données à caractère personnel vers ces pays, sont susceptibles d'avoir une incidence sur les conditions du partage ultérieur des informations collectées, et en particulier si les dispositions de ces accords internationaux peuvent avoir des répercussions sur l'application de la législation britannique en matière de protection des données, et si elles prévoient d'autres limitations ou exemptions en ce qui concerne l'utilisation et la divulgation à l'étranger d'informations collectées à des fins répressives. Le comité estime que ces informations et cette évaluation sont essentielles pour permettre un examen exhaustif du niveau de protection offert par le cadre législatif et les pratiques du Royaume-Uni en matière de divulgation à l'étranger.

2 INTRODUCTION

2.1 Le cadre britannique régissant la protection des données

12. Le cadre du Royaume-Uni en matière de protection des données est largement fondé sur celui de l'Union [en particulier la directive (UE) 2016/680 et le 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 (ci-après le «RGPD»)], 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 de 2018 sur la protection des données, qui est entrée en vigueur le 23 mai 2018 et a abrogé le UK Data Protection Act 1998 (loi britannique de 1998 sur la protection des données), transpose la directive (UE) 2016/680 en sa partie 3. En outre, elle précise l'application du RGPD dans le droit britannique, octroie 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»).

13. Comme indiqué au considérant 12 du projet de décision, le Gouvernement britannique a adopté le European Union (Withdrawal) Act 2018 [loi de 2018 sur l'Union européenne (retrait)], qui intègre la législation directement applicable de l'Union dans le droit britannique. Cette loi confère aux ministres britanniques le pouvoir d'introduire des dispositions de droit dérivé, au moyen d'instruments législatifs, pour apporter les modifications nécessaires aux dispositions du droit de l'Union appelées à rester en place à la suite du retrait du Royaume-Uni de l'Union européenne afin de les adapter au contexte national.

14. Par conséquent, le cadre juridique pertinent qui s'appliquera au Royaume-Uni au terme de la période de transition[7] se compose des instruments suivants:

Serious Crime (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 à des fins de lutte contre la grande criminalité), Washington DC, États-Unis, 3 octobre 2019.

[7] La période de transition est fixée au 31 décembre 2020, date à partir de laquelle le droit de l'Union ne s'appliquera plus au Royaume-Uni. La «période intermédiaire» est fixée au 30 juin 2021 au plus tard et désigne la période supplémentaire durant laquelle la transmission de données à caractère personnel depuis l'Union européenne vers le Royaume-Uni ne sera pas considérée comme un transfert.

- le United Kingdom General Data Protection Regulation (règlement général sur la protection des données du Royaume-Uni, ci-après le «RGPD britannique»), tel qu'intégré dans le droit du Royaume-Uni conformément au European Union (Withdrawal) Act 2018, tel que modifié par les DPPEC [Data Protection, Privacy and Electronic Communications (Amendment Etc.) (EU Exit) Regulations 2019 - règlements de 2019 sur la protection des données, le respect de la vie privée et les communications électroniques (modification, etc.) (sortie de l'UE), ci-après les «règlements DPPEC»];
- la loi de 2018 sur la protection des données, telle que modifiée par les règlements DPPEC de 2019, et les Data Protection, Privacy and Electronic Communications (Amendment Etc.) (EU Exit) Regulations 2020 [règlements de 2020 sur la protection des données, le respect de la vie privée et les communications électroniques (modifications, etc.) (sortie de l'UE)]; et
- l'Investigatory Power Act 2016 (loi de 2016 sur le pouvoir d'enquête, ci-après l'«IPA 2016»).

(ci-après collectivement dénommés le «cadre britannique en matière de protection des données»).

2.2 Portée de l'évaluation du CEPD

15. Le projet de décision de la Commission européenne est le fruit d'une évaluation du cadre britannique en matière de protection des données, ainsi que des discussions avec le gouvernement britannique qui ont suivi. Conformément à l'article 51, paragraphe 1, point g), de la directive (UE) 2016/680, le CEPD doit fournir un avis indépendant sur les conclusions de la Commission européenne, mettre en évidence les éventuelles lacunes du cadre d'adéquation, et s'efforcer de proposer des solutions pour y remédier.

16. Comme indiqué dans les critères de référence, «*les informations fournies par la Commission européenne devraient être exhaustives et permettre [*au CEPD] *d'évaluer l'analyse* […] *concernant le niveau de protection des données dans le pays tiers*»[8].

17. À cet égard, il convient d'observer que le CEPD n'a reçu en temps opportun qu'une partie des documents pertinents aux fins de l'examen du cadre juridique britannique. Il a obtenu la majeure partie de la législation britannique mentionnée dans le projet de décision par le biais de liens référencés dans ce document. La Commission européenne n'a pas été en mesure de fournir au comité les explications et les engagements écrits du Royaume-Uni pertinents pour cet exercice en rapport avec les échanges entre les autorités britanniques et la Commission européenne[9].

[8] Recommandations 01/2021 sur les critères de référence pour l'adéquation dans le cadre de la directive en matière de protection des données dans le domaine répressif, point 15, p. 5.

[9] Il s'agit des éléments pour lesquels la Commission européenne, dans son projet de décision, fait référence à des explications des autorités britanniques sans fournir les documents écrits desdites autorités contenant ces explications, notamment en ce qui concerne: les effets des dispositions transitoires et l'absence de clause de suppression automatique (considérant 87); des exemples de situations dans lesquelles le consentement peut servir de base appropriée pour le traitement (note de bas de page 68); l'utilisation des termes «incorrectes ou trompeuses» («incorrect or misleading») pour définir les données à caractère personnel «inexactes» («inaccurate») (note de bas de page 79); le mandat de l'ISC (Intelligence and Security Committee) (note de bas de page 245); le niveau peu élevé du seuil pour déposer une plainte auprès de l'IPT (Investigatory Powers Tribunal), et le fait qu'il n'est pas inhabituel que l'IPT détermine que le plaignant n'a en fait jamais fait l'objet d'une enquête par une autorité publique (note de bas de page 263); la combinaison des compétences découlant de la législation et de la common law (note de bas de page 52); les prérogatives exercées par le gouvernement (note de bas de page 62); le fait que d'autres organisations soient libres de suivre les principes du Code of Practice on the Management of Police Information (code de bonnes pratiques en matière de gestion des informations de police) si elles le souhaitent (note de bas de page 86).

18. Eu égard à ce qui précède et au délai limité (deux mois) dont il dispose pour adopter le présent avis, le CEPD a choisi de se concentrer sur certains points spécifiques présentés dans le projet de décision, et de présenter son analyse et son avis concernant ces points. 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, le CEPD a évidemment constaté que de nombreux aspects étaient substantiellement équivalents. Compte tenu de son rôle dans le processus d'adoption d'un constat d'adéquation ainsi que de la volumineuse législation et des nombreuses pratiques à analyser, le comité a décidé de concentrer son attention sur les aspects dont il a estimé qu'ils nécessitaient un examen plus approfondi.

19. Le CEPD a tenu compte du cadre européen applicable en matière de protection des données, et notamment des articles 7, 8 et 47 de la Charte des droits fondamentaux de l'Union européenne (ci-après «la charte»), qui protègent respectivement le droit au respect de la vie privée et familiale, le droit à la protection des données à caractère personnel et le droit à un recours effectif et à accéder à un tribunal impartial; ainsi que de 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 ce qui précède, le comité a examiné les exigences de la directive (UE) 2016/680, ainsi que la jurisprudence pertinente.

20. L'objectif de cet exercice est de fournir à la Commission européenne un avis sur l'évaluation du caractère adéquat du niveau de protection assuré au Royaume-Uni. Le concept de «niveau de protection adéquat», qui existait déjà dans le cadre de la directive 95/46/CE, a été renforcé 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»[10]. L'objectif n'est donc pas de refléter point par point la législation européenne, mais d'établir les exigences essentielles et fondamentales de la législation à 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 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 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[11].

2.3 Commentaires généraux et inquiétudes

2.3.1 Engagements internationaux du Royaume-Uni

21. Conformément à l'article 36, paragraphe 2, point c), de la directive (UE) 2016/680 et aux critères de référence[12], 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 sa participation à des systèmes multilatéraux ou régionaux,

[10] Voir arrêt de la CJUE du 6 octobre 2015, C-362/14, *Maximilian Schrems/Data Protection Commissioner*, EU:C:2015:650 (ci-après l'«arrêt *Schrems I*»), points 73 et 74.
[11] Voir les recommandations 01/2021 du CEPD sur les critères de référence pour l'adéquation dans le cadre de la directive en matière de protection des données dans le domaine répressif, point 14, p. 5.
[12] Voir les recommandations 01/2021 du CEPD sur les critères de référence pour l'adéquation dans le cadre de la directive en matière de protection des données dans le domaine répressif, point 24, p. 7.

en particulier en ce qui concerne la protection des données à caractère personnel, ainsi que de la mise en œuvre de ces obligations. Il convient également 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»)[13] et à son protocole additionnel[14].

22. **À cet égard, le CEPD se félicite que le Royaume-Uni ait adhéré à la CEDH et relève de la compétence de la Cour européenne des droits de l'homme (ci-après la «CouEDH»). Le Royaume-Uni a également adhéré à la convention 108 et à son protocole additionnel, a signé la convention 108+[15] en 2018 et œuvre actuellement à sa ratification.**

2.3.2 Possible divergence future du cadre britannique en matière de protection des données

23. Comme indiqué au considérant 171 du projet de décision, la Commission européenne doit tenir compte du fait qu'au terme de la période de transition prévue par l'accord de retrait[16], le Royaume-Uni administrera, appliquera et mettra en vigueur son propre régime de protection des données et que, dès que la disposition intermédiaire[17] prévue à l'article FINPROV.10A de l'accord de commerce et de coopération entre l'Union européenne et le Royaume-Uni[18] cessera de s'appliquer, il se peut, notamment, que des amendements ou des modifications soient apportés au cadre de protection des données examiné dans le projet de décision, ou que d'autres changements pertinents interviennent.

24. La Commission européenne a donc décidé d'inclure une clause de suppression automatique dans son projet de décision[19], qui fixe la date d'expiration quatre ans après son entrée en vigueur.

25. Il importe de faire remarquer que la possibilité pour les ministres et le Secrétaire d'État britanniques d'introduire des dispositions de droit dérivé après la fin de la période intermédiaire pourrait conduire, à l'avenir, à une divergence importante entre le cadre en matière de protection des données du Royaume-Uni et celui de l'Union.

26. Enfin, non seulement, depuis la fin de la période de transition, le Royaume-Uni n'est plus lié par la jurisprudence de la CJUE, mais les arrêts déjà adoptés par la Cour, considérés comme une jurisprudence retenue dans le cadre juridique britannique, pourraient ne plus lier le Royaume-Uni puisque, notamment, le Royaume-Uni a la possibilité de modifier le droit de l'Union retenu après la fin

[13] Voir la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, convention 108 du 28 janvier 1981.
[14] 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.
[15] Voir le Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ci-après la «convention 108+»), 18 mai 2018.
[16] 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).
[17] La période de transition est fixée au 31 décembre 2020, date à partir de laquelle le droit de l'Union ne s'appliquera plus au Royaume-Uni. La «période intermédiaire» est fixée au 30 juin 2021 au plus tard, et désigne la période supplémentaire durant laquelle la transmission de données à caractère personnel depuis l'Union européenne vers le Royaume-Uni ne sera pas considérée comme un transfert.
[18] 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).
[19] Voir article 4 du projet de décision. Voir également considérant 172 du projet de décision.

de la période intermédiaire et que sa Cour suprême n'est plus liée par une quelconque jurisprudence retenue de l'Union[20].

27. **Compte tenu des risques liés à un éventuel écart du cadre britannique en matière de protection des données par rapport à l'acquis de l'Union à la fin de la période intermédiaire, le CEPD se félicite de la décision de la Commission européenne d'introduire dans le projet de décision une clause de suppression automatique de quatre ans. Le comité tient toutefois à souligner ici l'importance du rôle de suivi de la Commission européenne[21]. Il convient, en effet, que celle-ci suive en permanence 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 transférées en vertu de la décision d'adéquation du Royaume-Uni, et ce dès son entrée en vigueur. La Commission doit également prendre les mesures appropriées en suspendant, en modifiant ou en abrogeant la décision d'adéquation, selon les circonstances, si, après l'adoption de ladite décision, elle dispose d'éléments indiquant que le Royaume-Uni ne garantit plus un niveau de protection adéquat.**

28. De son côté, le CEPD mettra tout en œuvre pour informer la Commission européenne de toute mesure pertinente prise par les autorités des États membres chargées du contrôle de la protection des données (ci-après les «autorités de contrôle»), en particulier en ce qui concerne les plaintes déposées par des personnes concernées dans l'Union européenne relatives au transfert de données à caractère personnel de l'Union vers le Royaume-Uni.

3 RÈGLES APPLICABLES AU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL PAR DES AUTORITÉS COMPÉTENTES À DES FINS RÉPRESSIVES

3.1 Champ d'application matériel

29. Le CEPD constate que les considérants 24 et suivants du projet de décision d'adéquation ne contiennent pas d'informations très détaillées sur les activités et le cadre juridique applicables aux agences exerçant des fonctions répressives autres que la police.

30. Par exemple, le UK Explanatory Framework for Adequacy Discussions (cadre explicatif relatif aux discussions sur l'adéquation du Royaume-Uni), section F: Law Enforcement[22], laisse entendre à la page 11 que la **National Crime Agency**(agence nationale de lutte contre la criminalité, ci-après la «NCA») pourrait être un organisme répressif présentant un intérêt particulier, qui dispose notamment d'une fonction plus large de renseignement criminel. La NCA décrit elle-même sa mission comme consistant à rassembler des renseignements à partir d'une diversité de sources de façon à optimiser les possibilités d'analyse, d'évaluation et de tactique, notamment par l'interception technique des communications et auprès de partenaires des services répressifs au Royaume-Uni et à l'étranger, des

[20] Voir article 6, paragraphes 3 à 6, EU (Withdrawal) Act 2018.
[21] Voir article 36, paragraphe 4, de la directive (UE) 2016/680.
[22] Voir le UK Government Explanatory Framework for Adequacy Discussions, section F: Law Enforcement, 13 mars 2020. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

agences de sécurité et de renseignement[23]. La NCA est également l'un des principaux interlocuteurs des partenaires internationaux en matière répressive et joue un rôle clé dans l'échange de renseignements criminels[24].

31. Le CEPD observe également que le Government Communications Headquarters (quartier-général des communications du gouvernement, ci-après le «GCHQ»), dont les activités relèvent généralement du champ d'application de la partie 4 de la loi de 2018 sur la protection des données, à savoir la sécurité nationale, joue aussi un rôle actif dans la lutte contre le préjudice sociétal et financier causé au Royaume-Uni par la grande criminalité organisée, en étroite collaboration avec le ministère de l'intérieur, la NCA, le HM Revenue and Customs (Recettes et douanes de Sa Majesté, ci-après le «HMRC») et d'autres services gouvernementaux[25]. Ses activités portent sur la lutte contre les abus sexuels sur des enfants, la fraude, d'autres types de criminalité économique, y compris le blanchiment d'argent, l'utilisation de la technologie à des fins criminelles, la cybercriminalité, la criminalité organisée en matière d'immigration, y compris la traite des êtres humains, ainsi que les drogues, les armes à feu et autres activités de contrebande illicites.

32. **Le CEPD invite la Commission européenne à compléter son analyse par une analyse des agences actives dans le domaine répressif qui semblent concentrer leurs opérations quotidiennes sur la collecte et l'analyse de données, y compris des données à caractère personnel, et plus particulièrement la NCA. Il l'invite également à examiner de plus près les agences telles que le GCHQ, dont les activités relèvent à la fois de la répression et de la sécurité nationale, ainsi que le cadre juridique qui s'applique à elles pour le traitement des données à caractère personnel.**

3.2 Garanties, droits et obligations

3.2.1 Traitement sur la base du «consentement» de la personne concernée

33. Le CEPD constate que la Commission européenne affirme, aux considérants 37 et 38 du projet de décision, que **le recours au consentement** n'est pas considéré comme pertinent dans un scénario d'adéquation, étant donné que, dans les situations de transfert, les données ne sont pas collectées

[23] Voir le site web 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.

[24] Bien que les renseignements traités par la NCA ne soient pas tous des données à caractère personnel, une grande partie de ces renseignements pourrait être constituée d'informations de ce type, et les activités décrites ici diffèrent de celles de la police classique, de sorte que l'évaluation de l'accès aux données à caractère personnel par les services répressifs du Royaume-Uni serait incomplète sans un examen approfondi des activités de la NCA. Il semble raisonnable de s'assurer que tous les services répressifs concernés ont la même conception des principes de protection des données, ce qui nous permettra de mieux comprendre le fonctionnement d'une agence telle que la NCA, dont le travail repose en grande partie sur les données. L'explication se poursuit dans la section «Looking to the future»: «Nous recherchons sans cesse de nouvelles possibilités de collecter, de développer et d'améliorer nos capacités d'accroître la quantité et la qualité des renseignements exploitables tant au Royaume-Uni qu'à l'étranger.» «À cette fin, nous développons la nouvelle capacité nationale d'exploitation des données, en utilisant les pouvoirs conférés à l'agence par le Crime and Courts Act, pour accéder aux données détenues par tous les services gouvernementaux, les exploiter et les relier entre elles.» […] «Ces efforts nous permettront d'accroître notre agilité et notre flexibilité pour répondre à de nouvelles menaces et agir de manière proactive, rassembler et analyser des informations et des renseignements sur les menaces émergentes, de façon à pouvoir prendre des mesures avant que les menaces se concrétisent.»

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

directement auprès d'une personne concernée par une autorité répressive britannique sur la base du consentement.

34. À cet égard, le comité rappelle que l'article 36, paragraphe 2, point a), de la directive (UE) 2016/680 impose d'examiner un large éventail d'éléments non limité à la situation de transfert, y compris «*l'état de droit, le respect des droits de l'homme et des libertés fondamentales, la législation pertinente, tant générale que sectorielle, y compris* […] *le droit pénal*».

35. Le consentement dans le contexte répressif peut constituer une base juridique pertinente pour le traitement des données, à titre de garantie supplémentaire ou plus généralement, de base pour l'exécution de pouvoirs d'enquête conduisant à l'acquisition de données à caractère personnel, par exemple le consentement d'un tiers à la perquisition de ses locaux ou à la confiscation du stockage de données.

36. Le CEPD observe, sur la base également des informations fournies par la Commission européenne au considérant 38 du projet de décision, que le recours au consentement, tel que défini dans le régime britannique, nécessiterait toujours de se fonder sur une base juridique. En d'autres termes, même si la police dispose du pouvoir légal de traiter les données aux fins d'une enquête, dans certaines circonstances particulières (par exemple, pour prélever un échantillon d'ADN), elle peut juger approprié de demander le consentement de la personne concernée.

37. **Le CEPD invite la Commission européenne à analyser, de manière générale, la possibilité de recourir au consentement dans un contexte répressif lors de l'évaluation du caractère adéquat d'un pays tiers dans le cadre de la directive (UE) 2016/680.**

3.2.2 Droits individuels

3.2.2.1 Certificats de sécurité nationale

38. Les responsables du traitement peuvent, en vertu de l'article 79 de la loi de 2018 sur la protection des données, demander des certificats de sécurité nationale délivrés par un ministre, un membre du Cabinet, l'Attorney General ou l'Advocate General pour l'Écosse attestant que les limitations des obligations et des droits consacrés aux chapitres 3 et 4 de la partie 3 de la loi de 2018 sur la protection des données constituent une mesure nécessaire et proportionnée à la protection de la sécurité nationale.

39. Ces certificats sont destinés à assurer aux responsables du traitement une plus grande sécurité juridique, et constitueront une preuve concluante du fait que la sécurité nationale s'applique lors du traitement de données à caractère personnel. Il convient toutefois de mentionner que ces certificats ne sont pas requis pour invoquer des restrictions en matière de sécurité nationale, mais constituent plutôt une mesure de transparence[26].

40. Le CEPD déduit de l'annexe 20 de la loi de 2018 sur la protection des données, articles 17 et 18, qu'un certificat de sécurité nationale délivré en vertu de la loi de 1998 sur la protection des données (ci-après l'«ancien certificat») a eu une efficacité prolongée en matière de traitement des données à caractère personnel au titre de la loi de 2018 sur la protection des données jusqu'au 25 mai 2019. Jusqu'à cette date, à moins qu'ils n'aient été remplacés ou révoqués, les anciens certificats étaient traités comme s'ils avaient été délivrés au titre de la loi de 2018 sur la protection des données. Toutefois, le comité

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

croit comprendre que, lorsqu'aucune date d'expiration expresse ne figure sur un certificat de sécurité nationale délivré en vertu de la loi de 1998 sur la protection des données, ledit certificat continuera de produire ses effets pour le traitement au titre de la loi de 1998 sur la protection des données, à moins que le certificat n'ait été révoqué ou annulé[27]. Bien que la protection conférée 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, le CEPD prend note du fait que de nouveaux certificats de sécurité nationale peuvent être délivrés au titre de la loi de 1998 sur la protection des données pour des données à caractère personnel traitées au titre de la loi de 1998 sur la protection des données[28].

41. **Dans un souci d'exhaustivité, le CEPD invite la Commission européenne à préciser, dans son projet de décision d'adéquation, que les certificats de sécurité nationale peuvent toujours être délivrés au titre de la loi de 1998 sur la protection des données. Il l'invite également à décrire dans son projet de décision d'adéquation les mécanismes de recours et de contrôle pour les certificats délivrés au titre de la loi de 1998 sur la protection des données. Enfin, le CEPD invite la Commission européenne à indiquer dans son projet de décision d'adéquation le nombre de certificats existants délivrés au titre de la loi de 1998 sur la protection des données, et à surveiller attentivement cet aspect.**

3.2.2.2 Prise de décision automatisée dans le cadre de la directive (UE) 2016/680

42. Le CEPD souligne que l'article 11, paragraphe 3, de la directive (UE) 2016/680 interdit tout profilage qui entraîne une discrimination à l'encontre des personnes physiques sur la base de catégories particulières de données à caractère personnel. Or, il constate que l'article 50 de la loi de 2018 sur la protection des données, qui définit les règles spécifiques applicables à la prise de décision automatisée, ne prévoit pas une telle interdiction.

43. **Le CEPD invite donc la Commission européenne à vérifier ce point et à faire explicitement état de ses conclusions dans sa décision d'adéquation. Il l'invite également à suivre de près les affaires liées à la prise de décision automatisée et au profilage.**

44. Selon les critères de référence, «*[l]a législation du pays tiers devrait, en tout état de cause, prévoir les garanties nécessaires pour les droits et libertés de la personne concernée. À cet égard, il convient également de tenir compte de l'existence d'un mécanisme permettant d'informer les autorités compétentes de l'État membre concerné de tout traitement ultérieur, tel que l'utilisation des données transférées aux fins d'un profilage à grande échelle*»[29].

45. **Le CEPD invite la Commission à examiner cet élément à la lumière des orientations données par le comité dans ses critères de référence.**

3.2.3 Transferts ultérieurs

46. Conformément aux critères de référence, les transferts ultérieurs de données à caractère personnel par le destinataire initial vers un autre pays tiers ou une organisation internationale ne doivent pas porter atteinte au niveau de protection, prévu dans l'Union, des personnes physiques dont les données sont transférées. Par conséquent, ces transferts ultérieurs de données ne devraient être autorisés que si la continuité du niveau de protection garanti par le droit de l'Union est assurée. Le CEPD considère que, comme la Commission européenne l'a indiqué dans son évaluation, les dispositions du chapitre 5 de la partie 3 de la loi de 2018 sur la protection des données, et en particulier son article 73, prévoient,

[27] Voir Home Office, The Data Protection Act 2018, National Security Certificates Guidance, August 2020, p. 5.
[28] Voir Home Office, The Data Protection Act 2018, National Security Certificates Guidance, August 2020, p. 5.
[29] Voir les recommandations 01/2021 du CEPD sur les critères de référence pour l'adéquation dans le cadre de la directive en matière de protection des données dans le domaine répressif, points 59 à 61.

en principe, un niveau de protection substantiellement équivalent à celui garanti par le droit de l'Union en ce qui concerne le transfert de données à caractère personnel d'une autorité répressive du Royaume-Uni vers un pays tiers.

47. Premièrement, l'article 73, paragraphe 1, point b), de la loi de 2018 sur la protection des données prévoit notamment qu'un responsable du traitement n'est pas autorisé à transférer des données à caractère personnel vers un pays tiers ou une organisation internationale, sauf si «*dans le cas où les données à caractère personnel ont été initialement transmises ou, de toute autre façon, mises à la disposition du responsable du traitement ou d'une autre autorité compétente par un État membre autre que le Royaume-Uni, cet État membre, ou toute personne établie dans cet État membre qui est une autorité compétente aux fins de la directive relative à la protection des données dans le domaine répressif, a autorisé le transfert conformément à la législation de l'État membre*». Ces dispositions semblent conformes aux critères de référence, selon lesquels il convient également de tenir compte de l'existence d'un mécanisme permettant aux autorités compétentes de l'État membre concerné d'être informées et d'autoriser un tel transfert ultérieur de données. Le destinataire initial des données transférées depuis l'UE devrait être responsable et pouvoir prouver que l'autorité compétente concernée de l'État membre a autorisé le transfert ultérieur et que des garanties appropriées sont prévues pour les transferts ultérieurs de données en l'absence d'une décision d'adéquation concernant le pays tiers vers lequel les données seraient transférées ultérieurement. «*Dans ce contexte, il convient de tenir compte de l'existence d'une obligation ou d'un engagement de mettre en œuvre les codes de traitement pertinents définis par les autorités des États membres de transfert*[30].»

48. **Le CEPD invite la Commission à examiner cet élément à la lumière des orientations données par le comité dans ses critères de référence.**

49. Deuxièmement, comme expliqué au considérant 81 du projet de décision, le Secrétaire d'État du Royaume-Uni a le pouvoir de reconnaître un pays tiers (ou un territoire, ou un secteur dans un pays tiers), une organisation internationale ou une description de ce pays, territoire, secteur ou organisation comme assurant un niveau adéquat de protection des données à caractère personnel, après consultation de l'ICO[31]. Lorsqu'il évalue le caractère adéquat du niveau de protection, le Secrétaire d'État doit tenir compte des mêmes éléments que ceux que la Commission est tenue d'apprécier au titre de l'article 36, paragraphe 2, points a) à c), de la directive (UE) 2016/680, interprété en combinaison avec son considérant 67 et la jurisprudence retenue de l'Union. Autrement dit, lors de l'évaluation du caractère adéquat du niveau de protection d'un pays tiers, le critère pertinent consistera à déterminer si ce pays tiers assure un niveau de protection «substantiellement équivalent» à celui qui est garanti au Royaume-Uni. Le CEPD prend bonne note de la capacité du Royaume-Uni, en vertu de la loi de 2018 sur la protection des données, de reconnaître des territoires comme offrant un niveau adéquat de protection des données au regard du cadre britannique en matière de protection des données, mais souligne toutefois que ces territoires pourraient ne pas bénéficier, à ce jour, d'une décision d'adéquation de la Commission européenne reconnaissant un niveau de protection «substantiellement équivalent» à celui garanti par l'Union européenne. Cela pourrait entraîner des risques pour la protection des données à caractère personnel transférées depuis l'Union européenne, en particulier si le cadre britannique en matière de protection des données devait s'écarter de l'acquis

[30] Voir les recommandations 01/2021 du CEPD sur les critères de référence pour l'adéquation dans le cadre de la directive en matière de protection des données dans le domaine répressif, points 55 et 56.

[31] Voir l'article 182, paragraphe 2, de la loi de 2018 sur la protection des données. Voir également le protocole d'accord sur le rôle de l'ICO en ce qui concerne les nouvelles évaluations du caractère adéquat au Royaume-Uni, 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/.

de l'Union à l'avenir. Il convient d'observer qu'en juillet 2020, l'arrêt rendu par la CJUE dans l'affaire *Schrems II*[32] a débouché sur l'invalidation de la décision relative au bouclier de protection des données UE-États-Unis, la CJUE ayant estimé que le cadre juridique américain ne pouvait pas être considéré comme offrant un niveau de protection substantiellement équivalent à celui de l'Union. Toutefois, les arrêts déjà adoptés par la CJUE, considérés comme une jurisprudence retenue dans le cadre juridique britannique, pourraient ne plus lier le Royaume-Uni puisque, en particulier, le Royaume-Uni a la possibilité de modifier le droit de l'Union retenu après la fin de la période intermédiaire, et que sa cour suprême n'est plus liée par une quelconque jurisprudence retenue de l'Union[33].

50. **Le CEPD invite donc la Commission européenne à suivre de près le processus et les critères d'évaluation de l'adéquation par les autorités britanniques à l'égard des autres pays tiers, en particulier les pays tiers qui ne sont pas reconnus par l'UE comme adéquats au regard de la directive (UE) 2016/680.**

51. Si la Commission européenne constate que le pays tiers jugé adéquat par le Royaume-Uni n'offre pas de niveau de protection substantiellement équivalent à celui garanti au sein de l'Union, conformément à l'article 36 de la directive (UE) 2016/680, **le CEPD invite la Commission européenne à prendre toutes les mesures nécessaires, comme, par exemple, la modification de la décision d'adéquation du Royaume-Uni afin d'y introduire des garanties spécifiques pour les données à caractère personnel provenant de l'Union européenne, et/ou à envisager la suspension de la décision d'adéquation du Royaume-Uni, lorsque les données à caractère personnel transférées depuis l'Union vers le Royaume-Uni font l'objet de transferts ultérieurs vers le pays tiers en question en vertu d'un règlement britannique en matière d'adéquation**.

52. **Enfin, en ce qui concerne les accords internationaux conclus, ou qui seront conclus à l'avenir, par le Royaume-Uni et l'éventuel accès, par les autorités de pays tiers partie(s) à de tels accords, à des données à caractère personnel de l'Union européenne, le CEPD recommande à la Commission européenne d'examiner l'interaction entre le cadre de protection des données du Royaume-Uni et ses engagements internationaux, en particulier 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'Union vers le Royaume-Uni en vertu d'une décision d'adéquation du Royaume-Uni; ainsi qu'à exercer un contrôle permanent et à prendre des mesures, le cas échéant, en ce qui concerne la conclusion d'accords internationaux entre le Royaume-Uni et des pays tiers qui risquent de porter atteinte au niveau de protection des données à caractère personnel prévu dans l'Union**. Par exemple, si la Commission européenne a mentionné le fait que l'accord Royaume-Uni/États-Unis sur la loi CLOUD[34] peut avoir une incidence sur les transferts ultérieurs depuis des fournisseurs de services du Royaume-Uni vers les États-Unis, **le CEPD souligne que l'entrée en vigueur de cet accord peut également avoir une incidence sur les transferts ultérieurs par les services répressifs britanniques,**

[32] Voir arrêt de la CJUE du 16 juillet 2020, C-311/18, *Data Protection Commissioner /Facebook Ireland Ltd et Maximilian Schrems*, EU:C:2020:559 (ci-après l'«arrêt *Schrems II*»).

[33] Voir article 6, paragraphes 3 à 6, de l'EU (Withdrawal) Act 2018.

[34] Voir Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime (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 à des fins de lutte contre la grande criminalité), Washington DC, États-Unis, 3 octobre 2019, https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019.

en particulier en ce qui concerne l'émission et la transmission d'ordres conformément à l'article 5 de l'accord Royaume-Uni/États-Unis sur la loi CLOUD.

53. Le comité estime également que la conclusion d'accords futurs avec des pays tiers aux fins de la coopération en matière répressive, qui constituent une base juridique pour le transfert de données à caractère personnel vers ces pays, peut également avoir des répercussions non négligeables sur les conditions du partage ultérieur des informations collectées, dès lors que ces accords peuvent avoir une incidence sur le cadre juridique britannique en matière de protection des données tel qu'il a été évalué.

54. **Le CEPD recommande dès lors à la Commission européenne de contrôler en permanence si la conclusion de futurs accords entre le Royaume-Uni et des pays tiers est susceptible d'avoir une incidence sur l'application de la législation britannique en matière de protection des données, et de prévoir une limitation ou une exemption supplémentaire en ce qui concerne le partage ultérieur ainsi que l'utilisation et la divulgation à l'étranger des informations recueillies à des fins répressives. Le comité estime que ces informations et cette évaluation sont essentielles pour permettre un examen exhaustif du niveau de protection offert par le cadre législatif et les pratiques du Royaume-Uni en matière de divulgation à l'étranger.**

55. Enfin, le CEPD observe que, en vertu de l'article 76, paragraphe 4, point b), de la loi de 2018 sur la protection des données (Transferts en raison de circonstances particulières), les services répressifs du Royaume-Uni peuvent transférer des données à caractère personnel vers un pays tiers ou une organisation internationale lorsque le transfert «*est nécessaire pour obtenir des avis juridiques en rapport avec l'une quelconque des finalités répressives*». **Le CEPD souligne que l'article 38 de la directive (UE) 2016/680 ne contient pas de disposition correspondante et invite dès lors la Commission européenne à préciser ce que l'on entend par «avis juridiques» et quel type de données à caractère personnel sont échangées dans de tels cas.**

3.2.4 Traitement ultérieur, y compris le partage ultérieur à des fins de sécurité nationale

56. Dans ses critères de référence, le CEPD avait indiqué que le traitement ou la divulgation ultérieurs de données transférées depuis l'Union à des fins autres que répressives, telles que des fins de sécurité nationale, devraient également être prévus par la loi, nécessaires et proportionnés. Comme l'a estimé la Commission européenne dans son projet de décision, l'article 36, paragraphe 3, de la loi de 2018 sur la protection des données, la Digital Economy Act 2017 (loi de 2017 sur l'économie numérique), la Crime and Courts Act 2013 (loi de 2013 sur la criminalité et les tribunaux), et la Serious Crime Act 2017 (loi de 2017 sur la grande criminalité) fournissent un cadre juridique clair permettant le partage ultérieur, à condition que celui-ci soit conforme aux règles énoncées dans la loi de 2018 sur la protection des données.

57. Le CEPD constate que, dans le contexte du traitement ultérieur à d'autres fins de données à caractère personnel transférées depuis l'Union européenne, la Commission européenne n'a pas évalué s'il existait des mécanismes permettant aux autorités répressives britanniques d'informer les autorités compétentes des États membres concernés d'un éventuel traitement ultérieur de données. Or, les critères de référence indiquent qu'il s'agit là d'un élément qui doit être pris en considération[35]. En outre, l'existence d'un tel mécanisme visant à informer les autorités compétentes des États membres

[35] Voir les recommandations 01/2021 du CEPD sur les critères de référence pour l'adéquation dans le cadre de la directive en matière de protection des données dans le domaine répressif, point 41 et note de bas de page 39.

concernés du traitement ultérieur des données à des fins répressives est également considérée comme un élément à prendre en compte en vertu des critères de référence[36].

58. **Le CEPD invite donc la Commission européenne à compléter son analyse par des informations sur l'existence de mécanismes permettant aux autorités répressives britanniques de notifier aux autorités compétentes des États membres concernés un éventuel traitement ultérieur de données transférées depuis l'Union européenne.**

59. En outre, en ce qui concerne le partage de données collectées par une autorité répressive avec un service de renseignement à des fins de sécurité nationale, la base juridique autorisant un tel partage est l'article 19 de la Counter-terrorism Act 2008 (loi de 2008 sur la lutte contre le terrorisme). À cet égard, le CEPD observe que le champ d'application et les dispositions de l'article 19 de cette loi ne sont pas examinés de façon exhaustive dans l'évaluation de la Commission européenne, et pourraient impliquer une utilisation plus large, en particulier en ce qui concerne l'article 19, paragraphe 2, qui dispose que «*[l]es informations obtenues par un service de renseignement dans le cadre de l'exercice de l'une de ses fonctions peuvent être utilisées par ce même service dans le cadre de l'exercice de l'une quelconque de ses autres fonctions*». À cet égard, le comité souligne que lors du traitement ou de la divulgation ultérieurs, les données devraient bénéficier du même niveau de protection que lors de leur traitement initial par l'autorité compétente destinataire.

3.3 Contrôle et application

60. Le CEPD observe que le contrôle des services répressifs en matière pénale est assuré par différents commissaires, en plus de l'ICO. Le projet de conclusions sur l'adéquation mentionne l'Investigatory Powers Commissioner (commissaire chargé des pouvoirs d'enquête, ci-après «IPC»), le Commissioner for the Retention and Use of Biometric Material (commissaire chargé de la conservation et de l'utilisation du matériel biométrique), ainsi que le Surveillance Camera Commissioner (commissaire chargé des caméras de surveillance). Dans ce contexte, il convient de faire remarquer que la CJUE a insisté à plusieurs reprises sur la nécessité d'un contrôle indépendant. L'IPC revêt une importance particulière en ce qui concerne l'accès aux données à caractère personnel transférées vers le Royaume-Uni. Le CEPD croit comprendre que l'IPC est un «commissaire judiciaire», comme les autres commissaires judiciaires, auquel il convient de se référer dans le cadre du chapitre sur la sécurité nationale, et que ces derniers jouissent de l'indépendance des juges, y compris lorsqu'ils exercent la fonction de commissaire. En ce qui concerne le bureau de l'IPC, la Commission européenne explique au considérant 245 du projet de décision qu'il fonctionne de manière autonome en tant qu'«organe indépendant», tout en étant financé par le ministère de l'Intérieur.

61. L'IPC est par ailleurs compétent pour le contrôle ex post des mesures de surveillance. Il semble toutefois que, pour cette fonction, le rôle de l'IPC consiste à formuler des recommandations en cas de non-respect et à informer la personne concernée, si l'erreur est grave et si l'information de la personne concernée est dans l'intérêt public.

62. Le CEPD n'a trouvé dans le projet de décision aucun autre élément indiquant la nécessité d'évaluer l'indépendance du commissaire chargé de la conservation et de l'utilisation du matériel biométrique et du commissaire chargé des caméras de surveillance.

63. **La Commission européenne est invitée à poursuivre l'examen de l'indépendance des commissaires judiciaires, y compris dans les cas où le commissaire n'exerce pas ou plus les fonctions de juge, ainsi**

[36] Voir les recommandations 01/2021 du CEPD sur les critères de référence pour l'adéquation dans le cadre de la directive en matière de protection des données dans le domaine répressif, point 40.

qu'à évaluer l'indépendance du commissaire chargé de la conservation et de l'utilisation de matériel biométrique et du commissaire chargé des caméras de surveillance.