

**Avis 26/2025 concernant le projet de décision d'exécution
de la Commission européenne constatant, conformément
au règlement (UE) 2016/679, le niveau de protection
adéquat des données à caractère personnel assuré par le
Royaume-Uni**

Adopté le 16 octobre 2025

Synthèse

Le 22 juillet 2025, la Commission européenne a entamé la procédure visant à l'adoption de son projet de décision d'exécution constatant le niveau de protection adéquat des données à caractère personnel assuré par le Royaume-Uni (RU), conformément à l'article 45, paragraphe 2, du RGPD. Ce projet de décision prolonge la validité de certaines parties de la précédente décision d'adéquation du 28 juin 2021 jusqu'en décembre 2031, à titre de référence.

Le même jour, la Commission européenne a demandé l'avis du comité européen de la protection des données (le «comité»). L'appréciation par le comité de l'adéquation 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.

Le comité s'est concentré à la fois sur l'évaluation des aspects généraux du projet de décision et sur l'accès des autorités publiques aux données à caractère personnel transférées depuis l'EEE vers le Royaume-Uni à des fins répressives et de sécurité nationale, y compris les voies de recours ouvertes aux personnes physiques au sein de l'EEE.

Le comité a également examiné si les garanties prévues par le cadre juridique du Royaume-Uni étaient en place et efficaces.

Le comité a utilisé comme référence principale pour ces travaux ses critères de référence pour l'adéquation avec le RGPD («les critères de référence») adoptés le 28 novembre 2017, tels que révisés et adoptés en dernier lieu le 6 février 2018, ainsi que les recommandations 02/2020 du comité européen de la protection des données sur les garanties essentielles européennes pour les mesures de surveillance.

Le comité se félicite de la poursuite de l'harmonisation entre le cadre de protection des données du Royaume-Uni et celui de l'UE, malgré les évolutions récentes du cadre juridique pertinent du Royaume-Uni. Dans ce contexte, le présent avis souligne plusieurs points qui requièrent une analyse plus approfondie, ainsi que certaines questions que la Commission devrait suivre de près dans les années à venir dans le cadre de l'obligation de suivi qui lui incombe en vertu de l'article 45, paragraphe 4, du RGPD.

Le comité note que le Royaume-Uni a introduit des modifications concernant le cadre juridique général «hérité» de l'UE en vertu de la *Retained EU Law (Revocation and Reform) Act 2023* [loi de 2023 sur le droit de l'UE maintenu en droit interne (révocation et réforme), la «loi REUL»], qui supprime, entre autres, le principe de primauté du droit de l'Union (avec des garanties pour certaines dispositions du RGPD) et l'application directe des principes du droit de l'Union, y compris le droit au respect de la vie privée et à la protection des données découlant de la Charte des droits fondamentaux. Le comité invite la Commission à apporter des explications et à engager une évaluation plus détaillée concernant les modifications apportées par la loi REUL, ainsi qu'à évaluer leur incidence sur le cadre juridique du Royaume-Uni en général et sur son cadre de protection des données en particulier. Le comité considère également qu'il s'agit d'un domaine qui devra faire l'objet d'un suivi étroit à l'avenir par la Commission.

Le comité constate que le secrétaire d'État s'est vu attribuer de nouveaux pouvoirs lui permettant d'apporter des modifications au nouveau cadre de protection des données par l'intermédiaire d'une réglementation dérivée, laquelle exige moins de contrôle parlementaire dans certains cas, par exemple concernant les transferts internationaux, la prise de décision automatisée et la

gouvernance de l'*Information Commission* (autorité britannique de protection des données, l'«ICO»). Le comité invite la Commission à mettre en évidence, dans la décision d'adéquation finale, les domaines qu'elle a l'intention de suivre attentivement, car il existe un risque que les divergences s'accroissent avec le droit de l'Union en matière de protection des données en raison du droit dérivé britannique.

Le comité remarque des modifications apportées aux règles régissant le transfert de données à caractère personnel, notamment la nouvelle liste indicative des éléments à prendre en considération dans le cadre du critère de l'adéquation, qui n'inclut pas certains éléments importants qui figuraient dans le précédent critère de l'adéquation pour le Royaume-Uni ⁽¹⁾. Cela s'applique à la fois aux transferts vers des pays tiers effectués dans le cadre du RGPD britannique et aux transferts de données traitées à des fins répressives. Le comité encourage la Commission à approfondir spécifiquement son évaluation à l'égard de ces aspects et à suivre les évolutions et la mise en œuvre pratique de ce nouveau critère de l'adéquation.

Le comité invite la Commission à procéder à une évaluation plus détaillée de la restructuration du *Information Commissioner's Office* (autorité britannique de protection des données, «ICO») en une commission et des règles de nomination et de révocation des membres exécutifs et non exécutifs de cette commission. Le comité demande également à la Commission à fournir davantage de détails sur la récente consultation de l'ICO, publiée après ce projet de décision, visant à introduire un nouveau système de triage pour le traitement des réclamations. Le comité invite la Commission à assurer le suivi de toutes ces modifications dès leur entrée en vigueur. Tout en notant avec satisfaction la politique de transparence de l'ICO et la disponibilité des données statistiques et analytiques de ses activités de contrôle de l'application de la législation, le comité invite également la Commission à procéder à une évaluation plus détaillée et à suivre l'application des pouvoirs en matière de mesures correctives et l'efficacité des sanctions et des voies de recours pour les parties concernées dans le cadre de protection des données du Royaume-Uni.

Le comité estime qu'il est essentiel d'évaluer les exemptions étendues concernant la sécurité nationale dans le cadre répressif et reste particulièrement vigilant à l'égard de toute exemption au principe de proportionnalité, ainsi qu'à l'égard de l'obligation de traiter les données à caractère personnel à des fins légitimes. De même, toute exemption aux pouvoirs de l'autorité de contrôle doit être abordée avec prudence. Toute limitation de l'exercice des droits et libertés reconnus par la Charte doit respecter leur contenu essentiel et, dans le respect du principe de proportionnalité, ne peut être apportée que si elle est nécessaire et répond effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui. Le comité invite la Commission à compléter son évaluation dans la décision d'adéquation finale et à surveiller spécifiquement l'application, dans la pratique, des exemptions concernant la sécurité nationale pour les autorités répressives.

Le comité note que les activités de traitement effectuées par les autorités répressives compétentes peuvent, dans certaines circonstances spécifiques, relever des règles normalement applicables au traitement des données à caractère personnel par les autorités nationales de sécurité. Dans ce contexte, il convient de veiller tout particulièrement à ce que le

⁽¹⁾ i) Les règles du pays tiers en ce qui concerne «la sécurité publique, la défense, la sécurité nationale et le droit pénal ainsi que l'accès des autorités publiques aux données à caractère personnel», ii) la jurisprudence, iii) l'existence de droits effectifs et opposables dont jouissent les personnes concernées et les voies de recours administratives et judiciaires que peuvent effectivement exercer les personnes concernées dont les données à caractère personnel sont transférées, et iv) une ou plusieurs autorités de contrôle indépendantes.

réfime de protection des données applicable au traitement des données à des fins de sécurité nationale ne soit pas étendu à des contextes sans rapport avec la sécurité nationale. Le comité invite la Commission à suivre si les autorités compétentes sont en mesure de maintenir une distinction claire entre les différentes finalités du traitement afin de se conformer au cadre juridique correspondant.

Le comité se félicite des clarifications obtenues entre le Royaume-Uni et les États-Unis dans le cadre de l'accord au titre de la loi américaine sur l'informatique en nuage (Cloud Act) entre ces deux pays, qui apportent une plus grande clarté juridique. Dans le même temps, le comité tient à rappeler la nécessité d'améliorer le niveau des garanties prévues par l'accord-cadre UE-États-Unis, dont les garanties en matière de respect de la confidentialité et de protection des données sont intégrées dans l'accord au titre de la loi américaine sur l'informatique en nuage (Cloud Act) conclu entre le Royaume-Uni et les États-Unis. Dans l'ensemble, le comité estime qu'il est nécessaire de clarifier l'évaluation, par la Commission, de l'accord au titre de la loi américaine sur l'informatique en nuage (Cloud Act) conclu entre le Royaume-Uni et les États-Unis, et de toute incidence éventuelle sur le niveau de protection. Le comité invite la Commission à continuer d'inclure l'accord au titre de la loi américaine sur l'informatique en nuage (Cloud Act) conclu entre le Royaume-Uni et les États-Unis dans ses futures évaluations et examens.

Comme récemment souligné dans la déclaration 5/2024, le comité considère que le chiffrement est essentiel pour garantir la sécurité et la confidentialité des données à caractère personnel et des communications électroniques. Les avis sur les capacités techniques au titre de l'IPA 2016, obligeant les entreprises à fournir une capacité de suppression du chiffrement à la demande du gouvernement, créent des vulnérabilités systémiques et constituent une menace directe pour l'intégrité et la confidentialité des communications électroniques. Ces évolutions méritent d'être prises en considération dans la décision d'adéquation, notamment au regard de l'article 45, paragraphe 2, point a), du RGPD, qui exige une évaluation non seulement du cadre juridique sur le papier, mais aussi de sa mise en œuvre, et devraient faire l'objet d'un suivi.

Le comité note que l'*Investigatory Powers Amendment Act 2024* (loi modificative de 2024 sur les pouvoirs d'enquête) a introduit un régime spécifique pour la conservation et l'examen d'ensembles de données à caractère personnel en masse pour lesquels les personnes physiques auxquelles se rapportent les données à caractère personnel «ne peuvent avoir aucune attente raisonnable en matière de confidentialité, ou seulement une attente raisonnable très limitée». Le comité estime que des précisions supplémentaires sont nécessaires concernant les modifications pertinentes, en particulier en ce qui concerne les notions d'«autorisation individuelles» et d'«autorisation par catégorie». En outre, le comité invite la Commission à suivre de près la mise en œuvre de l'expression «aucune attente raisonnable en matière de confidentialité, ou seulement une attente raisonnable très limitée» dans la pratique.

Table des matières

1. INTRODUCTION	7
1.1. Portée du projet de décision de la Commission	7
1.2. Champ d'application du présent avis du comité	8
1.3. Évolutions du cadre juridique britannique.....	9
1.4. Commentaires généraux et préoccupations	11
1.4.1. Engagements internationaux souscrits par le Royaume-Uni.....	11
1.4.2. Pouvoirs du secrétaire d'État d'apporter des modifications à la DUAA par l'intermédiaire d'une réglementation dérivée	11
2. Aspects généraux liés à la protection des données	12
2.1. Intérêts légitimes reconnus.....	12
2.1.1. Généralités	12
2.1.2. Divulcation aux fins du traitement décrit à l'article 6, paragraphe 1, point e.....	13
2.2. Droits individuels.....	14
2.2.1. Droits d'accès.....	14
2.2.2. Garanties applicables à l'«exemption en matière d'immigration»	15
2.3. Limitations relatives aux transferts ultérieurs	15
2.4. Prise de décision automatisée	17
2.4.1. Prise de décision automatisée et participation humaine	18
3. Mécanisme en matière de procédure et d'application	19
3.1. Contrôle et application	19
3.1.1. Contrôle par une autorité indépendante	19
3.1.2. Contrôle de l'application de la législation, y compris les sanctions	20
4. ACCÈS AUX DONNÉES À CARACTÈRE PERSONNEL TRANSFÉRÉES DEPUIS L'UNION EUROPÉENNE PAR LES AUTORITÉS PUBLIQUES au Royaume-Uni, ET UTILISATION DE CES DONNÉES.....	22
4.1. Accès aux données et utilisation de celles-ci par les autorités publiques du Royaume-Uni à des fins répressives	22
4.1.1. Bases juridiques et garanties applicables	23
4.1.1.1. Pouvoirs d'enquête à des fins répressives	23
4.1.1.2. Exemptions concernant la sécurité nationale pour les autorités répressives.....	23
4.1.2. Responsabilité conjointe du traitement entre les services de renseignement et les autorités répressives du Royaume-Uni.....	26

4.1.3.	Droit d'accès	27
4.1.4.	Transferts ultérieurs	27
4.1.4.1.	Un nouveau critère de protection des données	27
4.1.4.2.	Accord au titre de la loi américaine sur l'informatique en nuage (Cloud Act) conclu entre le Royaume-Uni et les États-Unis	28
4.1.5.	Contrôle et voies de recours	30
4.2.	Accès aux données et utilisation de celles-ci par les autorités publiques britanniques à des fins de sécurité nationale	31
4.2.1.	Utilisation des avis sur les capacités techniques	31
4.2.2.	Bases juridiques et garanties applicables	33
4.2.3.	Contrôle et voies de recours	35
5.	Examen, durée et renouvellement du projet de décision	36

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 (EEE) et, en particulier, son annexe XI et son protocole 37, tels que modifiés par la décision du Comité mixte de l'EEE n° 154/2018 du 6 juillet 2018 ⁽²⁾,

vu les articles 12 et 22 de son règlement intérieur,

A ADOPTÉ L'AVIS SUIVANT:

1. INTRODUCTION

1.1. Portée du projet de décision de la Commission

1. Le 22 juillet 2025, la Commission européenne (la «Commission») a demandé l'avis du Comité européen de la protection des données (le «comité») concernant le projet de décision d'exécution modifiant la décision d'exécution (UE) 2021/1772 de la Commission du 28 juin 2021 constatant, conformément au RGPD, le niveau de protection adéquat des données à caractère personnel assuré par le Royaume-Uni (le «projet de décision»). Dans son projet de décision, la Commission a conclu que le Royaume-Uni continuait d'assurer un niveau de protection adéquat des données à caractère personnel transférées de l'Union européenne vers le Royaume-Uni dans le cadre du champ d'application du RGPD.
2. Le comité note que ce projet de décision prolonge de six ans la validité de la décision d'exécution (UE) 2021/1772 de la Commission du 28 juin 2021 constatant, conformément au RGPD, le niveau de protection adéquat des données à caractère personnel assuré par le Royaume-Uni (la «précédente décision d'adéquation concernant le Royaume-Uni»), qui devait expirer le 27 juin 2025 (clause de caducité). La précédente décision d'adéquation concernant le Royaume-Uni avait été prolongée de six mois, jusqu'au 27 décembre 2025, en vertu de la décision (UE) 2025/1225 du 24 juin 2025, afin de permettre au Royaume-Uni de terminer ses réformes en matière de protection des données ⁽³⁾.
3. Dans son projet de décision, la Commission a évalué «si la conclusion selon laquelle le Royaume-Uni assure un niveau de protection adéquat des données à caractère personnel transférées de l'Union européenne vers le Royaume-Uni est toujours justifiée sur les plans factuel et juridique à

⁽²⁾ Dans le présent avis, on entend par «États membres» les «États membres de l'EEE».

⁽³⁾ Sur demande, le comité a publié l'«Avis 6/2025 concernant la prorogation des décisions d'exécution de la Commission européenne constatant le caractère adéquat du niveau de protection des données à caractère personnel assuré par le Royaume-Uni, adoptées au titre du règlement général sur la protection des données et de la directive en matière de protection des données dans le domaine répressif» (*Opinion 6/2025 regarding the extension of the European Commission Implementing Decisions under the GDPR and under the LED on the adequate protection of personal data in the United Kingdom*, disponible en anglais uniquement).

la lumière des développements intervenus depuis l'adoption de la précédente décision d'adéquation concernant le Royaume-Uni».

4. La Commission a axé son évaluation sur les nouvelles évolutions de la législation britannique en matière de protection des données, et notamment sur celles introduites par la *Data (Use and Access) Act 2025* [loi de 2025 sur les données (leur utilisation et l'accès à celles-ci), la «DUAA»]. La Commission a spécifiquement examiné les éléments énumérés au considérant 281 de la précédente décision d'adéquation concernant le Royaume-Uni, qui figurent tous dans le projet de décision.
5. Le comité convient que l'évaluation devrait principalement porter sur l'ensemble des nouvelles évolutions pertinentes de la législation britannique et sur les éléments mis en évidence dans la précédente décision d'adéquation concernant le Royaume-Uni, dans la mesure où tous les éléments énoncés à l'article 45, paragraphe 2, du RGPD sont évalués. Le comité apprécierait donc que, dans sa décision d'adéquation finale, la Commission précise de façon explicite que tous les éléments énumérés à l'article 45, paragraphe 2, du RGPD ont été évalués aux fins de conclure que le cadre juridique général du Royaume-Uni continue de garantir un niveau de protection adéquat des données à caractère personnel transférées de l'Union européenne vers le Royaume-Uni. Le comité souhaiterait également que la Commission précise qu'elle évaluera ces éléments de manière continue dans le cadre de son rôle de suivi.

1.2. Champ d'application du présent avis du comité

6. Le comité doit rendre à la Commission un avis indépendant en ce qui concerne l'évaluation du caractère adéquat du niveau de protection assuré par un pays tiers ⁽⁴⁾, recenser les insuffisances du cadre d'adéquation, le cas échéant, et s'efforcer de formuler des propositions pour y remédier ⁽⁵⁾. En raison de la situation spécifique du Royaume-Uni, la nouvelle décision d'adéquation complète la décision d'adéquation de 2021, qui reste valable pour les parties qui ne sont pas spécifiquement abordées dans ce projet de décision. De même, dans le présent avis, le comité européen de la protection des données s'appuie sur son avis 14/2021 et le développe plus avant ⁽⁶⁾. Par conséquent, l'analyse et les observations du CEPD fournies dans son avis précédent concernant la précédente décision d'adéquation concernant le Royaume-Uni restent, en règle générale, pertinentes.
7. Compte tenu de ce qui précède, le comité a concentré ses observations sur certains points présentés dans le projet de décision, en particulier lorsque des éclaircissements supplémentaires, davantage d'informations ou un suivi futur par la Commission européenne sont nécessaires.

⁽⁴⁾ Voir article 70, paragraphe 1, point s), du RGPD.

⁽⁵⁾ Voir Groupe de travail «Article 29», Critères de référence pour l'adéquation, chapitre 2 Aspects procéduraux des décisions d'adéquation dans le cadre du RGPD, adoptés le 28 novembre 2017, tels que révisés et adoptés en dernier lieu le 6 février 2018, WP254 rev.01 (approuvés par le comité, voir <https://edpb.europa.eu/our-worktools/general-guidance/endorsed-wp29-guidelines>); (ci-après les «Critères de référence pour l'adéquation avec le RGPD»).

⁽⁶⁾ 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, https://www.edpb.europa.eu/system/files/2021-04/edpb_opinion142021_ukadequacy_gdpr.pdf_en.pdf.

8. Le comité note également que, conformément aux articles 47 et 94 du règlement (UE) 2018/1725 ⁽⁷⁾, les institutions, organes et organismes de l'Union européenne peuvent transférer des données à caractère personnel vers un pays tiers, un territoire, un secteur ou une organisation internationale reconnus par la Commission européenne, en vertu de l'article 45, paragraphe 3, du RGPD, comme assurant un niveau de protection adéquat, à condition que le transfert ait lieu exclusivement pour permettre l'exécution des missions qui relèvent de la compétence du responsable du traitement, sans qu'une autorisation supplémentaire soit nécessaire. Le comité invite la Commission à rappeler cette possibilité juridique dans les considérants de la décision d'adéquation finale.

1.3. Évolutions du cadre juridique britannique

9. Comme expliqué dans le projet de décision ⁽⁸⁾, à l'issue de la période de mise en œuvre convenue dans l'accord sur le retrait du Royaume-Uni de l'Union européenne ⁽⁹⁾ le 31 décembre 2020, le Royaume-Uni avait l'intention d'adopter un nouveau régime de protection des données qui s'écarterait du cadre juridique de l'UE. En fin de compte, le Royaume-Uni a apporté des modifications limitées à son cadre de protection des données existant, notamment en vertu de la DUAA.
10. Au-delà de la protection des données, l'un des changements les plus importants apportés au cadre juridique britannique depuis l'adoption de la précédente décision d'adéquation concerne le cadre juridique général «hérité» de l'UE (appelé «droit de l'UE maintenu en droit interne»), c'est-à-dire les dispositions juridiques intégrées dans le droit britannique par l'intermédiaire de la *European Union (Withdrawal) Act 2018* (loi de 2018 relative au retrait de l'Union européenne). Le droit de l'UE maintenu englobait les principes généraux du droit de l'Union, y compris les droits fondamentaux découlant de la Charte des droits fondamentaux de l'Union européenne [la «Charte»⁽¹⁰⁾] et les principes de proportionnalité et de nécessité, qui ont eu une influence sur le développement et l'interprétation du droit de la protection des données au Royaume-Uni. En vertu de la loi de 2018 relative au retrait de l'Union européenne, le droit de l'UE maintenu en droit interne avait conservé sa primauté par rapport au droit dérivé britannique et il devait être interprété conformément aux principes généraux du droit de l'Union. Cependant, depuis l'introduction de la *Retained EU Law (Revocation and Reform) Act 2023* [loi de 2023 sur le droit de l'UE maintenu en droit interne (révocation et réforme), la «loi REUL»] ⁽¹¹⁾, le Royaume-Uni a supprimé l'application directe des principes du droit de l'Union européenne dans son droit interne, y compris des droits fondamentaux découlant de la Charte. La loi REUL a également supprimé le principe de primauté du droit européen, car le droit de l'UE maintenu en droit interne (désormais appelé «droit assimilé») doit désormais être interprété de manière compatible avec le droit national britannique, et non conformément aux principes du droit de l'UE. Cela constitue un changement important dans l'ordre juridique britannique.
11. En outre, bien qu'actuellement en suspens, un nouveau critère juridique plus souple permettant aux juges de la Cour d'appel et de la Cour suprême de s'écarter de la jurisprudence de l'Union

⁽⁷⁾ Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE (le «règlement (UE) 2018/1725») (JO L 295 du 21.11.2018, p. 39).

⁽⁸⁾ Voir le considérant 2 du projet de décision.

⁽⁹⁾ La période de mise en œuvre est une période convenue dans l'accord sur le retrait du Royaume-Uni de l'Union européenne, pendant laquelle le Royaume-Uni ne sera plus membre de l'UE, mais continuera à être soumis aux règles de l'UE et restera membre du marché unique et de l'union douanière. Voir la loi de 2020 relative à l'accord de retrait de l'Union européenne.

⁽¹⁰⁾ Charte des droits fondamentaux de l'Union européenne (JO C 326 du 26.10.2012, p. 391–407).

⁽¹¹⁾ Voir le considérant 11 du projet de décision.

pourrait être introduit en vertu de la loi REUL ⁽¹²⁾. Ce changement, s'il est adopté, pourrait constituer un tournant au Royaume-Uni.

12. Malgré ces changements, le comité se félicite de l'inclusion de garanties dans la loi REUL afin de veiller à ce que la législation relative à la protection des données ne soit pas supplantée dans certaines circonstances. Ces garanties comprennent l'exigence selon laquelle tout acte législatif «qui impose une obligation, ou confère un pouvoir, de traiter des données à caractère personnel ne prévaut pas sur une exigence prévue par la législation principale en matière de protection des données relative au traitement des données à caractère personnel» et que le cadre de protection des données continue de prévaloir sur d'autres actes législatifs britanniques ⁽¹³⁾. Néanmoins, le comité note que ces garanties comprennent également deux exceptions : i) le Parlement britannique peut choisir de déroger délibérément aux exigences en matière de protection des données ⁽¹⁴⁾ et ii) certaines dispositions de la DPA 2018 sont exemptées et, en tant que telles, prévaudront sur le RGPD britannique ⁽¹⁵⁾. Les implications de la deuxième exemption restent incertaines et font l'objet de débats au Royaume-Uni.
13. En ce qui concerne la protection des droits fondamentaux consacrés dans la Charte, le considérant 12 du projet de décision explique que toutes les références aux droits et libertés fondamentaux dans le RGPD britannique et la DPA 2018 ont été remplacées par des références aux droits prévus par la Convention européenne des droits de l'homme, incorporés dans la législation nationale en vertu de la *Human Rights Act 1998* (loi de 1998 sur les droits de l'homme) ⁽¹⁶⁾.
14. Le comité invite la Commission à procéder à une évaluation plus détaillée de ces modifications de l'ordre juridique britannique décrites aux paragraphes 10, 11 et 12 ci-dessus afin d'explicitier les modifications apportées par la loi REUL et d'évaluer leur incidence sur le cadre de protection des données du Royaume-Uni. Le comité considère également qu'il s'agit là d'un domaine qui devra faire l'objet d'un suivi étroit de la part de la Commission à l'avenir et invite celle-ci à agir en ce sens.
15. Enfin, le comité note plusieurs changements apportés par la DUAA au cadre juridique applicable aux communications électroniques, y compris aux cookies, et rappelle que le traitement des données à caractère personnel pourrait déclencher le champ d'application matériel du RGPD britannique ⁽¹⁷⁾. Par conséquent, il invite la Commission à inclure ces questions dans son évaluation en vue de la décision finale dans la mesure où elles pourraient avoir une incidence sur la protection des données. Le comité demande en outre à la Commission de suivre avec attention l'effet pratique des modifications liées aux cookies exemptés de consentement.

⁽¹²⁾ Voir l'article 6 des *The Retained EU Law (Revocation and Reform) Act 2023 (Commencement No. 2 and Saving Provisions) (Revocation) Regulations 2024* [règlements de 2024 en vertu de la loi REUL (entrée en vigueur n° 2 et exceptions (révocation))].

⁽¹³⁾ Voir l'article 183A de la loi DPA 2018, tel qu'introduit par l'article 106, paragraphe 2, de la DUAA.

⁽¹⁴⁾ Voir l'article 183(A), paragraphe 3, de la DPA 2018, tel qu'introduit par l'article 106, paragraphe 2, de la DUAA.

⁽¹⁵⁾ Ces dispositions sont énumérées à l'article 186, paragraphe 3, de la DPA 2018. Cela signifie qu'en cas de conflit entre l'article 23 du RGPD britannique et l'un des articles cités, par exemple l'annexe 2 de la DPA 2018 contenant les exemptions relatives aux droits des personnes concernées, l'interprétation de la DPA 2018 prévaudra.

⁽¹⁶⁾ Voir l'article 8 de la Convention européenne des droits de l'homme.

⁽¹⁷⁾ Comité européen de la protection des données, avis 5/2019 relatif aux interactions entre la directive «vie privée et communications électroniques» et le RGPD, en particulier en ce qui concerne la compétence, les missions et les pouvoirs des autorités de protection des données, adopté le 12 mars 2019, disponible à l'adresse suivante: https://www.edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf.

1.4. Commentaires généraux et préoccupations

1.4.1. Engagements internationaux souscrits par le Royaume-Uni

16. En ce qui concerne les engagements internationaux souscrits par le Royaume-Uni ⁽¹⁸⁾, le comité se félicite que le Royaume-Uni continue d'adhérer à la CEDH et de relever de la compétence de la Cour européenne des droits de l'homme. En outre, le Royaume-Uni a également adhéré à la convention 108 ⁽¹⁹⁾ et à son protocole additionnel ⁽²⁰⁾, et a signé la Convention 108+ ⁽²¹⁾ en 2018. Ces engagements internationaux constituent des considérations importantes ⁽²²⁾ et il devrait en être tenu compte dans le cadre de l'évaluation aux fins du renouvellement des décisions d'adéquation concernant le Royaume-Uni au titre du RGPD et de la directive en matière de protection des données dans le domaine répressif.
17. Dans l'ensemble, le comité soutient les efforts visant à une ratification rapide de la convention 108+ par les pays tiers, car il s'agit d'une mesure importante en vue de l'alignement sur les principes reconnus à l'échelle internationale en matière de protection des données et d'un signe de leur engagement en faveur de normes plus larges et du respect des droits fondamentaux.

1.4.2. Pouvoirs du secrétaire d'État d'apporter des modifications à la DUAA par l'intermédiaire d'une réglementation dérivée

18. Bien que la plupart des modifications apportées au cadre de protection des données du Royaume-Uni visent à clarifier et à faciliter le respect de la législation, certaines peuvent, en fonction de leur mise en œuvre, avoir une incidence sur le niveau de protection des données à caractère personnel au Royaume-Uni.
19. À cet égard, le comité note que le secrétaire d'État s'est vu attribuer de nouveaux pouvoirs lui permettant d'apporter des modifications à la DUAA par l'intermédiaire d'une réglementation dérivée, qui exige un contrôle parlementaire moindre. Dans certains cas, par exemple les transferts internationaux (voir article 2.3), la prise de décision automatisée (article 2.4) et la gouvernance de l'IC (article 3), ces nouveaux pouvoirs sont étendus et le projet de décision ne fournit aucune information supplémentaire sur les garanties qui seront mises en place et la manière dont ces pouvoirs seront utilisés dans la pratique.
20. Le comité invite la Commission à mettre en évidence, dans la décision d'adéquation finale, les domaines qu'elle a l'intention de suivre attentivement, car il existe un risque que les divergences s'accroissent avec le droit de l'Union en matière de protection des données en raison du droit dérivé britannique.

⁽¹⁸⁾ Voir chapitre 1: informations générales relatives au concept d'adéquation des critères de référence pour l'adéquation.

⁽¹⁹⁾ Voir la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Convention 108, 28 janvier 1981.

⁽²⁰⁾ 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.

⁽²¹⁾ Voir le Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel («Convention 108+»), 18 mai 2018.

⁽²²⁾ Voir le considérant 105 du RGPD.

2. Aspects généraux liés à la protection des données

2.1. Intérêts légitimes reconnus

2.1.1. Généralités

21. Dans les considérants 22, 23 et 24, la Commission concentre son évaluation sur l'introduction d'une nouvelle base juridique, à savoir le traitement nécessaire aux fins d'un intérêt légitime reconnu. L'annexe 1 du RGPD britannique mis à jour dresse une liste de ces intérêts légitimes reconnus.
22. Selon les orientations de l'ICO à cet égard ⁽²³⁾, les responsables du traitement des données qui s'appuient sur un intérêt légitime reconnu comme base juridique restent tenus de se conformer à toutes les autres exigences du RGPD britannique, y compris de veiller à ce que le traitement soit nécessaire et proportionné pour atteindre la finalité préalablement approuvée. Étant donné que cela n'est pas rappelé dans le projet de décision et constitue un élément essentiel aux fins de pouvoir conclure que cette nouvelle base juridique ne porte pas atteinte au niveau de protection des droits des personnes concernées, le comité invite la Commission à clarifier ce point.
23. Le fait d'énumérer les intérêts légitimes reconnus dans la loi ne semble pas poser de problème en soi, pas plus que la décision d'introduire cette nouvelle base juridique, qui apporte davantage de clarté aux responsables du traitement et devrait être saluée.
24. Toutefois, le comité constate que certains intérêts légitimes reconnus consistent en: i) la nécessité de traiter des données à caractère personnel à des fins de préservation de la sécurité nationale, de protection de la sécurité publique ou pour des raisons de défense («condition relative à la sécurité nationale, à la sécurité publique et à la défense»); ii) la nécessité de traiter des données à caractère personnel pour détecter une infraction, enquêter sur celle-ci ou la prévenir («condition relative à la criminalité»); et iii) la «divulcation aux fins du traitement décrit à l'article 6, paragraphe 1, point e»).
25. En ce qui concerne la «condition relative à la sécurité nationale, la sécurité publique et la défense» et la «condition relative à la criminalité», le comité note que le projet de décision ne contient aucune information supplémentaire concernant l'utilisation pratique de ces bases juridiques par les responsables du traitement et les sous-traitants. Le comité apprécierait que la Commission fournisse davantage de détails sur les informations et garanties supplémentaires reçues de la part des autorités compétentes britanniques concernant l'application pratique de cette base juridique et invite la Commission à en suivre l'application.
26. Le comité note également que l'ICO travaille à l'élaboration d'orientations spécifiques sur cette question, qui, au moment du présent avis, comprennent une définition de ces concepts. Compte tenu de l'importance d'obtenir des clarifications concernant ces concepts, le comité invite la Commission à suivre de près l'élaboration des orientations de l'ICO.

⁽²³⁾ Voir les orientations de l'ICO concernant les intérêts légitimes, disponibles à l'adresse suivante: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/legitimate-interests/>.

2.1.2. Divulgarion aux fins du traitement décrit à l'article 6, paragraphe 1, point e

27. Le comité fait remarquer que l'intérêt légitime reconnu nouvellement établi, qui autorise «la divulgation aux fins du traitement décrit à l'article 6, paragraphe 1, point e», introduit la possibilité de partager des données à caractère personnel avec les autorités publiques sur une base volontaire. Comme l'ICO le précise dans ses orientations récentes ⁽²⁴⁾, cet intérêt légitime reconnu ne confère pas en soi aux autorités requérantes un droit d'accès aux données à caractère personnel, mais un responsable du traitement peut invoquer cet intérêt préalablement approuvé lorsque les autorités indiquent qu'elles ont besoin de données pour l'exécution de leurs missions ou fonctions publiques. Le comité constate également que ces demandes de divulgation introduites dans le cadre d'une mission d'intérêt public peuvent non seulement concerner des informations à caractère personnel destinées à être utilisées à des fins couvertes par le RGPD britannique, mais également des finalités de traitement relevant des parties 3 et 4 de la DPA 2018. Par conséquent, cette modification est également pertinente en ce qui concerne l'accès du gouvernement à des fins répressives et de sécurité nationale ⁽²⁵⁾.
28. Dans ce contexte, la question se pose de savoir les critères que le responsable du traitement doit évaluer afin de décider s'il convient de fournir volontairement des données en réponse à une demande d'informations. En particulier, comme l'indique l'ICO dans ses orientations ⁽²⁶⁾, le comité comprend que le critère de nécessité relatif à cette condition de l'intérêt légitime reconnu diffère des autres conditions spécifiées à l'annexe 1. Pour les demandes de divulgation introduites dans le cadre d'une mission d'intérêt public, la nécessité signifie que le responsable du traitement doit examiner le traitement nécessaire avant de divulguer les informations à caractère personnel demandées. Le responsable du traitement doit déterminer si les informations qu'il souhaite partager sont proportionnées et nécessaires pour répondre à la demande. En revanche, le critère de nécessité ne s'étend pas à la question de savoir si les données à caractère personnel sont réellement nécessaires à l'exécution de la mission ou de la fonction d'intérêt public, étant donné que le responsable du traitement peut s'appuyer sur la déclaration du demandeur selon laquelle celui-ci a besoin des informations à caractère personnel concernées pour une mission d'intérêt public spécifique ⁽²⁷⁾. En fait, bien souvent, et notamment lorsque des demandes sont formulées à des fins répressives ou de sécurité nationale, le responsable du traitement ne sera pas en mesure de procéder à une telle évaluation.
29. Dans ce contexte, le comité invite la Commission à suivre de près l'application pratique de cette disposition.
30. De l'avis du comité, les services répressifs et les autorités nationales de sécurité ne devraient pas utiliser ce mécanisme pour contourner les restrictions juridiques existantes s'imposant à leurs pouvoirs contraignants en matière de collecte de données ou pour obtenir plus de données que ce qui est strictement nécessaire à l'accomplissement de leurs missions. En outre, le comité estime qu'il est important que les responsables du traitement tiennent compte des orientations de l'ICO sur la manière de valider une demande de divulgation introduite dans le cadre d'une

⁽²⁴⁾ Voir note de bas de page 23.

⁽²⁵⁾ Voir les orientations de l'ICO sur les conditions relatives aux demandes de divulgation introduites dans le cadre d'une mission d'intérêt public, disponibles à l'adresse suivante: <https://ico.org.uk/for-organisations/recognised-legitimate-interest-guidance/what-are-the-recognised-legitimate-interest-conditions/public-task-disclosure-request-condition/>.

⁽²⁶⁾ Voir note de bas de page 23.

⁽²⁷⁾ Voir note de bas de page 23.

mission d'intérêt public et invite la Commission à inclure cet aspect dans l'examen périodique de la décision ⁽²⁸⁾.

2.2. Droits individuels

31. Le comité prend acte de l'analyse de la Commission selon laquelle des modifications limitées ont été apportées dans le domaine des droits individuels. Celles-ci incluent les modifications apportées à l'article 12 et un nouvel article 12A du RGPD britannique qui fournissent davantage de précisions sur les délais de réponse aux demandes des personnes concernées ⁽²⁹⁾. En outre, l'article 13, paragraphe 5, du RGPD britannique prévoit une dérogation au droit à l'information si des données à caractère personnel sont traitées à des fins de recherche scientifique ou historique, sous réserve de garanties supplémentaires prévues à l'article 84B du RGPD britannique. Le comité considère que ces deux modifications ne portent pas atteinte au niveau de protection essentiellement équivalent prévu par le RGPD britannique.

2.2.1. Droits d'accès

32. L'article 15, paragraphe 1A, du RGPD britannique introduit une évaluation de la proportionnalité, telle qu'elle est développée dans la jurisprudence nationale du Royaume-Uni. En particulier, les responsables du traitement ne doivent effectuer que des « recherches raisonnables et proportionnées » afin de répondre aux demandes d'accès.
33. Le comité constate qu'une telle évaluation de la proportionnalité n'est pas prévue dans le cadre de protection des données de l'UE, qui ne prévoit aucune réserve générale quant à la proportionnalité eu égard aux efforts que le responsable du traitement doit engager pour se conformer à la demande des personnes concernées en vertu de l'article 12 du RGPD, mais fournit uniquement des motifs de refus dans son paragraphe 5 ⁽³⁰⁾.
34. Par conséquent, selon le comité, il est important de définir de manière adéquate la notion de « recherches raisonnables et proportionnées », qui devrait être interprétée de manière restrictive et suffisamment uniforme. Les responsables du traitement devraient avoir une compréhension cohérente de ce qui est « raisonnable et proportionné », qu'elle soit fondée sur la jurisprudence ou sur les orientations d'une autorité de contrôle, car l'application de cette notion pourrait potentiellement conduire à des normes différentes en matière de respect du droit d'accès, en particulier en fonction du niveau des mesures techniques et organisationnelles mises en place par le responsable du traitement pour traiter les demandes d'accès. Le comité apprécierait que la Commission fournisse des informations plus détaillées sur l'interprétation des termes « recherches raisonnables et proportionnées » sur la base des orientations et de la jurisprudence

⁽²⁸⁾ Dans ses orientations sur les conditions relatives aux demandes de divulgation introduites dans le cadre d'une mission d'intérêt public (voir note de bas de page 25), l'ICO précise que les responsables du traitement devraient, par exemple, exiger que la demande soit établie par écrit et procéder à des vérifications pour s'assurer de l'authenticité de la demande ou de l'autorité dont dispose le salarié de l'organisation pour agir en son nom.

⁽²⁹⁾ Notamment en raison de la nécessité de confirmer l'identité de la personne concernée ou du paiement de frais.

⁽³⁰⁾ Article 12, paragraphe 5, du RGPD: «Aucun paiement n'est exigé pour fournir les informations au titre des articles 13 et 14 et pour procéder à toute communication et prendre toute mesure au titre des articles 15 à 22 et de l'article 34. Lorsque les demandes d'une personne concernée sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif, le responsable du traitement peut: a) exiger le paiement de frais raisonnables qui tiennent compte des coûts administratifs supportés pour fournir les informations, procéder aux communications ou prendre les mesures demandées; ou b) refuser de donner suite à ces demandes. Il incombe au responsable du traitement de démontrer le caractère manifestement infondé ou excessif de la demande.»

nationales disponibles. Dans ce contexte, le comité invite la Commission à veiller à ce que le droit d'accès ne soit pas indûment limité.

2.2.2. Garanties applicables à l'«exemption en matière d'immigration»

35. L'ancienne «exemption en matière d'immigration»⁽³¹⁾ permettait aux responsables du traitement participant au «contrôle de l'immigration» de restreindre certains droits des personnes concernées prévus par la DPA 2018, si ceux-ci étaient susceptibles de nuire à certaines activités de contrôle de l'immigration⁽³²⁾. En raison des remises en cause de la légalité de cette exemption au moment de l'adoption de la précédente décision d'adéquation concernant le Royaume-Uni, le traitement des données à caractère personnel au titre de l'exemption a été exclu du champ d'application de cette décision.
36. Depuis la précédente décision d'adéquation concernant le Royaume-Uni, l'exemption en matière d'immigration a été complétée à deux reprises par des garanties⁽³³⁾. Elle inclut désormais les garanties suivantes: i) elle ne doit être invoquée qu'au cas par cas, ii) les droits et libertés de la personne concernée et les vulnérabilités potentielles sont pris en considération, iii) le secrétaire d'État tient un registre de l'utilisation de l'exemption en matière d'immigration et informe généralement la personne concernée de son utilisation et iv) l'utilisation de l'exemption en matière d'immigration est limitée au traitement par le secrétaire d'État (y compris le ministère de l'intérieur du Royaume-Uni et ses agences). En outre, l'exercice de mise en balance nécessaire afin de déterminer si l'exercice des droits de la personne concernée est susceptible de nuire à l'efficacité du contrôle de l'immigration a été détaillé. L'ICO a également publié des orientations détaillées sur l'utilisation de l'exemption. Dans ses orientations, l'ICO a confirmé l'interprétation restrictive de l'exemption et précisé que les restrictions au titre de l'exemption en matière d'immigration ne devaient s'appliquer que de manière sélective à certains droits spécifiques des personnes concernées. Il a également déclaré que, lors de la réalisation du test de mise en balance, les responsables du traitement doivent s'assurer que le risque pesant sur le contrôle de l'immigration est substantiel et l'emporte sur le risque pour les intérêts de la personne.
37. Le comité prend acte de l'analyse détaillée de la Commission. Dans le contexte des difficultés juridiques qui ont précédé ces changements, le comité encourage la Commission à surveiller leur application future.

2.3. Limitations relatives aux transferts ultérieurs

38. Le comité se félicite de l'attention continue accordée par la Commission à l'application pratique des règles du Royaume-Uni relatives aux transferts de données à caractère personnel vers des pays tiers et encourage la Commission à maintenir et à approfondir cet engagement. Ce point est particulièrement pertinent en ce qui concerne le pouvoir du secrétaire d'État de promulguer de nouveaux règlements ciblés afin d'approuver des transferts (i) vers un secteur ou une zone géographique spécifique au sein d'un pays tiers; (ii) vers un responsable du traitement ou un sous-traitant spécifique; (iii) vers un destinataire spécifique des données à caractère personnel; (iv) de certains types spécifiques de données à caractère personnel; (v) effectués par

³¹ Voir l'annexe 2 de la DPA 2018, partie 1 de la version précédente de la DPA.

⁽³²⁾ Voir les paragraphes 61 et 62 de l'avis 14/2021 du comité: «nuire au maintien d'un contrôle efficace de l'immigration» ou «la détection d'activités qui pourraient nuire au maintien d'un contrôle efficace de l'immigration, ou aux enquêtes en la matière».

⁽³³⁾ Par voie réglementaire en 2022 ainsi qu'en 2024.

certaines moyens spécifiques; ou (vi) sur la base de la législation, de programmes, de listes ou d'autres dispositions ou documents pertinents, tels qu'ils sont en vigueur à tout moment; et de conférer un pouvoir discrétionnaire à une personne [article 45A, paragraphe 4, du RGPD britannique].

39. Le comité comprend que l'article 45A, paragraphe 4, du RGPD britannique vise à permettre une certaine souplesse dans l'approbation de transferts spécifiques. Par exemple, en ce qui concerne les points ii) et iii), le comité comprend qu'ils pourraient couvrir les transferts vers des entités privées dans un pays tiers. Cela signifierait que ces entités privées s'engagent à se conformer au critère de la protection des données. Il n'apparaît pas clairement comment le secrétaire d'État évaluerait, dans la pratique, que certains responsables du traitement établis dans un pays tiers — qui n'est pas considéré comme adéquat — peuvent se conformer au critère de la protection des données (par exemple, en ce qui concerne les voies de recours). De même, la manière dont le critère de protection des données serait mis en œuvre pour l'article 45A, paragraphe 4, points iv) et v), du RGPD britannique n'est pas claire.
40. Le comité apprécierait que la Commission fournisse davantage de détails sur les informations et garanties supplémentaires reçues en ce qui concerne l'application pratique du critère relatif à la protection des données et qu'elle explique son évaluation quant à la manière dont le niveau de protection est maintenu dans de telles situations ⁽³⁴⁾. Le comité invite également la Commission à suivre de près l'évolution de l'application de cette disposition.
41. En outre, le comité comprend, à la lecture des informations supplémentaires fournies par la Commission, que le critère de l'«opportunité de faciliter les transferts de données à caractère personnel à destination et en provenance du Royaume-Uni» n'est pas un élément du critère de protection des données, mais simplement un facteur supplémentaire que le secrétaire d'État peut examiner lorsque les exigences liées au critère sont pleinement remplies. Le comité invite la Commission à clarifier ce point dans sa décision finale sur l'adéquation, car le texte de la loi n'est pas tout à fait clair à ce sujet, ainsi qu'à suivre les implications pratiques et la mise en œuvre de ce critère.
42. En ce qui concerne le nouveau critère de protection des données introduit par la DUAA ⁽³⁵⁾, le comité constate que la nouvelle liste indicative d'éléments à prendre en considération dans le critère de l'adéquation n'est pas exhaustive et que le nouveau critère de l'adéquation prévoit que le niveau de protection des personnes concernées dans les pays tiers ou les organisations internationales destinataires n'est «pas sensiblement inférieur» à la norme prévue pour les personnes concernées par la législation pertinente du Royaume-Uni en matière de protection des données. Cette liste supprime des éléments essentiels qui figuraient dans le précédent critère de l'adéquation du Royaume-Uni et qui jouaient un rôle important dans l'évaluation de la question de savoir si un pays tiers offre un niveau de protection des données à caractère personnel essentiellement équivalent. Le nouveau critère ne fait plus référence i) aux règles du pays tiers en ce qui concerne «la sécurité publique, la défense, la sécurité nationale et le droit pénal ainsi que l'accès des autorités publiques aux données à caractère personnel», ii) à la jurisprudence (le nouveau critère fait désormais référence à «la constitution, aux traditions et à la culture du pays»), iii) à l'existence de droits effectifs et opposables dont jouissent les personnes concernées et les voies de recours administratives et judiciaires que peuvent effectivement exercer les personnes concernées dont les données à caractère personnel sont

⁽³⁴⁾ Voir l'article 45A, paragraphe 4 du RGPD britannique.

⁽³⁵⁾ Voir le considérant 42 du projet de décision.

transférées [le nouveau critère fait désormais référence à b) l'existence et aux pouvoirs d'une autorité chargée de faire appliquer la protection des personnes concernées à l'égard du traitement des données à caractère personnel dans le pays ou par l'organisation, c) des voies de recours juridictionnel ou non juridictionnel pour les personnes concernées dans le cadre de ce traitement], et iv) à une ou plusieurs autorités de contrôle indépendantes (le nouveau critère fait désormais référence à une «autorité chargée de faire appliquer la protection des personnes concernées à l'égard du traitement des données à caractère personnel dans le pays ou par l'organisation»).

43. Bien qu'il soit reconnu que les critères de référence pour l'adéquation avec le RGPD ne fournissent que des détails limités sur cet aspect, le comité rappelle sa référence au fait que «le niveau de protection des personnes physiques dont les données sont transférées ne doit pas être compromis par le transfert ultérieur»⁽³⁶⁾, ce qui ne peut être interprété comme excluant la nécessité d'une autorité de contrôle indépendante et de droits effectifs et opposables pour les personnes concernées.
44. Le comité encourage la Commission à approfondir davantage son évaluation sur ces aspects. Une telle clarification apporterait une grande sécurité juridique et contribuerait à renforcer la confiance dans l'instrument d'adéquation. Le comité invite également la Commission à suivre de près l'évolution de la situation et la mise en œuvre pratique du nouveau critère
45. En ce qui concerne la qualité de membre (associé) du Royaume-Uni au CBPR, le comité note que la qualité de membre actuelle n'implique aucune facilitation des transferts de données du Royaume-Uni vers d'autres membres du forum CBPR. Le comité salue la position adoptée par la Commission à cet égard, notamment son engagement à continuer de suivre de près les évolutions futures dans ce domaine, en particulier si le Royaume-Uni a l'intention de devenir membre à part entière, et rappelle que les pays membres du CBPR ne sont pas reconnus comme garantissant un niveau de protection suffisant pour les données à caractère personnel provenant de l'UE.

2.4. Prise de décision automatisée

46. Le comité prend note de l'article 80 de la DUAA (introduisant les articles 22A à 22D du RGPD britannique), qui apporte des modifications importantes au cadre régissant la prise de décision automatisée, en particulier lorsqu'elle repose sur le traitement de catégories de données non spéciales. Avant l'adoption de la DUAA, l'article 22 du RGPD britannique reprenait le cadre de protection des données de l'UE, avec une interdiction générale de la prise de décision automatisée assortie d'exceptions limitées.
47. L'article 22B, paragraphe 1, du RGPD britannique interdit le traitement de catégories particulières de données à caractère personnel pour les décisions fondées exclusivement sur un traitement automatisé qui ont des effets juridiques ou des effets d'une importance similaire pour la personne concernée, à certaines exceptions près (Article 22B, paragraphes 2 et 3, du RGPD britannique, y compris lorsque le traitement est fondé sur le consentement, un contrat ou est requis par la loi).

⁽³⁶⁾ Voir chapitre 3: Principes généraux en matière de protection des données visant à garantir que le niveau de protection dans un pays tiers, un territoire ou un ou plusieurs secteurs déterminés au sein de ce pays tiers ou d'une organisation internationale est substantiellement équivalent à celui garanti par la législation européenne, des critères de référence pour l'adéquation avec le RGPD.

48. Le comité observe que cette interdiction ne s'applique pas lorsque les responsables du traitement prennent des décisions importantes à l'aide de processus automatisés fondés sur des catégories de données non spéciales, à moins que la base juridique du traitement ne soit un intérêt légitime reconnu, conformément à l'article 6, paragraphe 1, point ea), du RGPD britannique.
49. La loi met désormais l'accent non plus sur la restriction de l'utilisation de la prise de décision automatisée, mais sur la mise en place de garanties pour les décisions importantes. Ces garanties comprennent i) la fourniture d'informations à la personne concernée sur le processus décisionnel, ii) la possibilité pour celle-ci de présenter des observations sur la décision ⁽³⁷⁾, iii) la possibilité de contester cette décision ainsi que iv) la possibilité pour la personne concernée de demander l'intervention humaine du responsable du traitement. Le comité note que, bien que cette nouvelle approche s'écarte du cadre juridique précédent, l'article 22C du RGPD britannique exige des responsables du traitement qu'ils mettent en œuvre des garanties appropriées garantissant un niveau adéquat de protection des personnes concernées.
50. Compte tenu de l'évolution rapide de l'environnement réglementaire et des progrès réalisés dans le domaine des technologies automatisées, telles que l'IA, le comité encourage la Commission à étendre, dans sa décision d'adéquation finale, son évaluation des incidences pratiques envisagées de cette nouvelle approche, qui doit encore être testée dans la pratique, ainsi qu'à surveiller sa mise en œuvre.

2.4.1. Prise de décision automatisée et participation humaine

51. Le comité se félicite de la clarification apportée concernant la signification de la prise de décision automatisée et de l'intervention humaine. L'article 22A du RGPD britannique précise qu'une décision fondée uniquement sur un traitement automatisé signifie qu'il n'y a aucune intervention humaine significative dans le processus décisionnel. Les responsables du traitement sont également tenus d'évaluer dans quelle mesure le profilage contribue à une décision afin de déterminer si l'intervention humaine était significative.
52. En outre, l'article 22D du RGPD britannique confère au secrétaire d'État le pouvoir de préciser, par voie réglementaire, s'il existe ou non une participation humaine significative à la prise de la décision décrite dans le règlement. De même, le secrétaire d'État est également habilité à déterminer si la décision décrite dans le règlement est considérée ou non comme ayant un effet similaire significatif sur les personnes concernées.
53. La portée et la marge d'appréciation de ces pouvoirs ne sont pas claires. Par conséquent, le comité invite la Commission à analyser ces nouveaux pouvoirs conférés au secrétaire d'État et à suivre toute évolution à cet égard. D'autre part, les pouvoirs supplémentaires conférés au secrétaire d'État en ce qui concerne les garanties requises par l'article 22C du RGPD britannique constituent un changement bienvenu, car ils viendront s'ajouter et/ou compléter les garanties déjà requises et permettront de déterminer ce qui est insuffisant en matière de garanties.

⁽³⁷⁾ C'est-à-dire fournir des informations et des arguments supplémentaires, ce qui ne constitue pas encore un recours officiel.

3. Mécanisme en matière de procédure et d'application

3.1. Contrôle et application

3.1.1. Contrôle par une autorité indépendante

54. Le comité note qu'avec l'entrée en vigueur de la DUAA⁽³⁸⁾, l'ICO, qui était auparavant structuré comme une personne morale individuelle, va être transformé en une nouvelle structure par l'intermédiaire de la création d'une personne morale constituée en société (une commission), à savoir l'*Information Commission* (ICO), conformément à l'article 148 et à l'annexe 12A de la DPA 2018.
55. Le comité observe que la restructuration d'une autorité, qui cesse d'être une personne morale individuelle et devient une personne morale constituée en société, n'affecte pas en soi l'indépendance de l'autorité et l'efficacité de son action en matière d'application des lois. Il convient de prêter attention à d'autres éléments tels que les règles relatives à la nomination et à la révocation, et à cet égard, le comité se félicite que seule Sa Majesté puisse révoquer le président de l'ICO à la suite d'une recommandation des deux chambres du Parlement britannique en cas de faute grave.
56. Les règles détaillées relatives au travail et au fonctionnement du nouvel IC figurent à l'annexe 12A de la DPA 2018. Ce document régit, entre autres, le cadre structurel et organisationnel de l'ICO, les conditions requises pour la nomination de ses membres exécutifs et non exécutifs ainsi que des autres membres du personnel (employés et comité externe) et comprend des dispositions relatives à la durée du mandat, à la rémunération, à la gestion des comptes et au licenciement. Les points 5 et 6 de l'annexe 12A⁽³⁹⁾ contiennent des règles et des garanties qui doivent être respectées lors de la nomination de membres non exécutifs et qui pourraient être pertinentes pour la mise en place de l'organisme et son indépendance (par exemple, la sélection au mérite et les conflits d'intérêts).
57. Le comité note que le projet de décision ne fournit aucun détail sur les changements apportés au fonctionnement et à l'organisation de la nouvelle autorité chargée de la protection des données. De plus, il n'y a pas de détails sur la procédure de nomination et de révocation des membres exécutifs et non exécutifs. Étant donné que ces éléments sont pertinents pour l'évaluation du mécanisme de contrôle, le comité invite la Commission à décrire plus en détail les changements et l'évaluation y afférente, notamment en ce qui concerne la structure et l'organisation de l'ICO, la nomination et la révocation de ses membres, y compris de ses membres non exécutifs.
58. En ce qui concerne l'indépendance de l'IC, le comité note qu'en vertu de l'article 6 de l'annexe 12A de la DPA 2018, les conflits d'intérêts peuvent empêcher une nomination par le secrétaire d'État en tant que président ou membre non exécutif de l'ICO. Définissant plus avant l'expression «conflit d'intérêts», l'article 6, paragraphe 5 fait référence à «un intérêt financier ou autre susceptible de nuire à l'exercice par la personne de sa fonction de membre de la Commission». En ce qui concerne l'indépendance des membres de l'IC, un tel «autre intérêt», par exemple une proximité économique spéciale et/ou des relations d'affaires, peut également indiquer des conflits d'intérêts et devrait être pris en compte dans le processus de nomination des membres

³⁸ Voir la partie 6 «The Information Commission», DUAA n° 117, pages 133 et suivantes.

⁽³⁹⁾ Voir l'annexe 12A de la DPA 2018.

de l'ICO. Le comité invite donc la Commission à vérifier que les restrictions s'appliquent dans la pratique.

59. En ce qui concerne les objectifs actualisés que l'ICO doit prendre en compte dans l'exécution de ses tâches et dans l'élaboration de sa stratégie, tels que, entre autres, la promotion de l'innovation et de la concurrence (article 120B de la DPA 2018), la Commission rappelle que «de même, le droit de l'Union en matière de protection des données établit également un équilibre entre la protection des données à caractère personnel et plusieurs autres droits et objectifs fondamentaux», et cite les considérants 2 et 4, ainsi que l'article 23 du RGPD. Le comité reconnaît que la protection des données n'est pas un droit absolu et doit être mise en balance avec d'autres droits et objectifs fondamentaux, conformément au principe de proportionnalité. Toutefois, le comité observe que les considérants 2 et 4 du RGPD, ainsi que son article 23, diffèrent d'une disposition juridique exigeant expressément des autorités chargées de la protection des données qu'elles tiennent compte d'une série d'objectifs dans l'exercice de leurs fonctions. Dans un souci de clarté, le comité invite la Commission à reformuler ce considérant afin d'éviter de donner l'impression que les considérants 2 et 4, ainsi que l'article 23 du RGPD, ont la même signification que l'article 120B de la DPA 2018, et à veiller à ce que la mise en œuvre de ces objectifs actualisés dans la pratique n'entraîne pas un déséquilibre excessif au détriment du droit à la protection des données à caractère personnel qui porterait atteinte au niveau de protection des données à caractère personnel.

3.1.2. Contrôle de l'application de la législation, y compris les sanctions

60. Le comité se félicite du fait que la disposition contenue dans le précédent projet de loi visant à réformer le cadre de protection des données du Royaume-Uni [le «Data Protection and Digital Information Bill» (projet de loi sur la protection des données et les informations numériques) ⁽⁴⁰⁾] et prévoyant que l'ICO doit tenir compte de l'avis du secrétaire d'État dans l'exercice de ses pouvoirs, ne figure plus dans le nouveau cadre de protection des données.
61. Le comité considère également comme positif le fait que, depuis l'adoption de la précédente décision d'adéquation concernant le Royaume-Uni, l'ICO ait publié de nombreux codes de pratiques, lignes directrices, avis et autres documents d'orientation utiles à l'intention des parties concernées.
62. Comme dans son avis 14/2021 ⁽⁴¹⁾, le comité souligne qu'un mécanisme de contrôle efficace permettant une enquête indépendante sur les réclamations, ainsi que des voies de recours administratives et judiciaires efficaces, sont des éléments essentiels pour déterminer si un système de protection des données assure un niveau de protection adéquat. En outre, l'existence de sanctions effectives joue un rôle important s'agissant de garantir le respect des règles.
63. Dans ce contexte, le comité attire l'attention de la Commission sur la consultation publique publiée par l'ICO le 22 août concernant ses propositions de traitement des réclamations ⁽⁴²⁾, qui

⁽⁴⁰⁾ Voir l'article 32, nouvel article 120, points E, F, G, H du projet de loi sur la protection des données et les informations numériques.

⁽⁴¹⁾ Voir avis 14/2021 du comité, paragraphes 112 à 114.

⁽⁴²⁾ Voir la consultation de l'ICO sur les projets de modification concernant la manière dont sont traitées les réclamations en matière de protection des données: <https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/2025/08/ico-consultation-on-draft-changes-to-how-we-handle-data-protection-complaints/>; <https://ico.org.uk/media2/nrljbhr2/proposed-dpt-framework-20250822.pdf>

n'a été lancée qu'après l'adoption du projet de décision de la Commission. Dans son introduction⁽⁴³⁾ aux propositions soumises à la consultation publique, l'ICO indique qu'il s'attend à ce que, une fois la DUAA entrée en vigueur, davantage de réclamations soient résolues par les organisations elles-mêmes sans l'intervention de l'ICO. Cette évaluation de l'ICO s'explique par le fait que la DUAA impose aux organisations de nouvelles exigences aux fins d'introduire une procédure de réclamation portant spécifiquement sur des questions de protection des données. L'article 164A de la DPA 2018⁽⁴⁴⁾ dispose que les responsables du traitement doivent prendre des mesures pour aider les personnes physiques qui souhaitent introduire une réclamation concernant l'utilisation de leurs données à caractère personnel. Par exemple, ils doivent leur fournir un formulaire de réclamation qui peut être rempli par voie électronique et par d'autres moyens, ils doivent accuser réception des réclamations dans un délai de 30 jours et, «sans retard injustifié», prendre les mesures appropriées pour répondre à la réclamation et informer l'auteur de la réclamation de l'issue de celle-ci. Si les réclamations doivent être traitées par l'ICO, les propositions présentées en vue d'une consultation publique devraient servir de base au traitement des réclamations par l'ICO. À cet égard, l'ICO propose une sorte de système de triage, selon lequel les réclamations doivent être traitées avec des priorités et des résultats différents. Cela devrait permettre à l'ICO, en tant qu'autorité de régulation stratégique, de concentrer ses ressources sur les risques les plus importants et d'identifier les problèmes systémiques à un stade plus précoce. La proposition de l'ICO établit une liste non exhaustive de critères susceptibles d'augmenter ou de diminuer la probabilité qu'une réclamation fasse l'objet d'un suivi⁽⁴⁵⁾.

64. Les changements décrits au paragraphe 57 peuvent entraîner une modification de l'approche adoptée par l'ICO en matière de traitement des réclamations. En raison du lancement de la consultation publique après la publication du projet de décision de la Commission, ces modifications n'ont pas encore été prises en considération dans le projet de décision.
65. Le comité invite la Commission à inclure cet élément dans son évaluation et à assurer un suivi, en particulier, des résultats de la consultation publique de l'ICO. En outre, le comité demande à la Commission de suivre de près le traitement futur des réclamations par l'ICO afin de garantir le maintien d'un niveau de protection équivalent.
66. Le comité note en outre que les pouvoirs réglementaires étendus conférés au secrétaire d'État par la DUAA, y compris le pouvoir d'adopter des dispositions juridiques, peuvent entraîner des conséquences sur le fonctionnement des travaux de l'ICO et de ses membres. Le comité renvoie, par exemple, à la nécessité pour l'ICO de consulter le secrétaire d'État en ce qui concerne certaines de ses tâches. En particulier, l'article 124A de la DPA 2018⁽⁴⁶⁾ impose à l'ICO d'établir des codes de pratiques appropriés contenant des lignes directrices pour le traitement approprié des données à caractère personnel, lorsque cela est requis par un règlement adopté par le secrétaire d'État. L'ICO est tenu de consulter le secrétaire d'État avant de modifier ou d'élaborer ces codes.
67. Compte tenu de l'importance de l'indépendance de l'ICO, le comité invite la Commission à suivre de près ces nouveaux pouvoirs du secrétaire d'État, notamment leur effet pratique sur les travaux de l'ICO.

⁽⁴³⁾ Voir note de bas de page 41.

⁽⁴⁴⁾ Voir l'article 164A de la DPA 2018.

⁽⁴⁵⁾ Voir note de bas de page 41.

⁽⁴⁶⁾ Code de pratique pour le traitement des données à caractère personnel.

68. Comme l'a déjà souligné le comité dans son avis 14/2021, l'ICO dispose bien des pouvoirs nécessaires, qui correspondent étroitement aux pouvoirs des autorités de contrôle des États membres de l'UE énoncés à l'article 58 du RGPD. Parallèlement, comme l'a déjà souligné le comité, l'existence de sanctions effectives joue un rôle important s'agissant de garantir le respect des règles. Le comité invite la Commission à procéder à une évaluation plus approfondie et à contrôler l'application des pouvoirs en matière de mesures correctives et l'efficacité des sanctions et des voies de recours pour les parties concernées dans le cadre de protection des données du Royaume-Uni ⁽⁴⁷⁾.

4. ACCÈS AUX DONNÉES À CARACTÈRE PERSONNEL TRANSFÉRÉES DEPUIS L'UNION EUROPÉENNE PAR LES AUTORITÉS PUBLIQUES au Royaume-Uni, ET UTILISATION DE CES DONNÉES

69. Le projet de décision se concentre sur les évolutions pertinentes pour l'évaluation du niveau de protection au Royaume-Uni depuis l'adoption de la précédente décision d'adéquation concernant le Royaume-Uni, laquelle reste valable pour les aspects du cadre de protection des données du Royaume-Uni qui n'ont pas été modifiés ou qui ne sont pas concernés. Cette approche générale couvre également l'analyse de la Commission concernant l'accès aux données à caractère personnel et leur utilisation par les autorités publiques au Royaume-Uni. Cet aspect spécifique est souvent appelé «accès des autorités publiques» et constitue l'un des éléments énumérés à l'article 45, paragraphe 2, point a), du RGPD que la Commission doit prendre en considération pour déterminer si le niveau de protection est essentiellement équivalent.
70. Dans ce contexte, les sections suivantes traitent d'un certain nombre de points spécifiques soulevés dans le projet de décision actuellement à l'examen qui sont pertinents en ce qui concerne les données à caractère personnel transférées depuis l'EEE en vertu de la décision d'adéquation du RGPD britannique et auxquelles les autorités publiques du Royaume-Uni ont accès et qu'elles traitent, y compris les transferts ultérieurs. L'analyse et les commentaires formulés par le comité dans son avis 14/2021 ⁽⁴⁸⁾ restent globalement valables.

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

71. Le cadre de protection des données régissant l'accès et l'utilisation à des fins répressives par les autorités publiques du Royaume-Uni a fait l'objet de modifications législatives depuis la dernière évaluation de la Commission figurant dans la précédente décision d'adéquation concernant le Royaume-Uni. Ces modifications découlent notamment de la *National Security Act 2023* (loi de 2023 sur la sécurité nationale), de l'*Investigatory Powers Amendment Act 2024* (loi modificative de 2024 sur les pouvoirs d'enquête) et de l'introduction de la DUAA. Ce dernier point est également abordé dans le projet de décision de la Commission modifiant la décision d'exécution (UE) 2021/1773, ainsi que

⁽⁴⁷⁾ Voir l'avis 14/2021 du comité européen de la protection des données, paragraphe 113.

⁽⁴⁸⁾ Voir l'avis 14/2021 du comité.

dans l'avis correspondant du comité, rendu sur la base de l'article 51, paragraphe 1, point g), de la directive en matière de protection des données dans le domaine répressif.

4.1.1. Bases juridiques et garanties applicables

4.1.1.1. Pouvoirs d'enquête à des fins répressives

72. Dans les considérants 81 à 85 du projet de décision, la Commission expose les modifications apportées à l'*Investigatory Powers Act 2016* (loi de 2016 sur les pouvoirs d'enquête, «IPA 2016») par l'*Investigatory Powers Amendment Act 2024* (loi modificative de 2024 sur les pouvoirs d'enquête), dans la mesure où elles concernent le traitement des données à des fins répressives ⁽⁴⁹⁾. Dans l'ensemble, la Commission fournit des informations détaillées. En ce qui concerne une modification spécifique, le comité estime toutefois que le projet de décision gagnerait à être clarifié davantage.
73. La loi modificative de 2024 sur les pouvoirs d'enquête a introduit une révision de la définition du terme «opérateur de télécommunications», c'est-à-dire les destinataires potentiels d'un avis de conservation en vertu de l'IPA 2016 ⁽⁵⁰⁾. La définition modifiée inclut désormais toute personne qui «contrôle ou fournit un système de télécommunication qui (i) n'est pas (entièrement ou partiellement) situé au Royaume-Uni ou contrôlé depuis le Royaume-Uni, et (ii) est utilisé par un tiers pour offrir ou fournir un service de télécommunication à des personnes au Royaume-Uni». Bien que la Commission se réfère aux notes explicatives de la loi modificative de 2024 sur les pouvoirs d'enquête, indiquant que l'article 261, paragraphe 10, point c) «apporte des précisions supplémentaires garantissant que les grandes entreprises ayant des structures d'entreprise complexes sont couvertes dans leur intégralité par l'IPA 2016», et que «la modification [...] ne cherche pas à inclure d'autres entreprises dans le champ d'application», les implications de ce changement restent floues, par exemple, quant à la question de savoir si elle élargirait le volume de données à caractère personnel potentiellement soumises à un avis de conservation. Le comité invite donc la Commission à examiner plus en détail les effets de cette modification et à suivre spécifiquement cet aspect, notamment à la lumière des principes de nécessité et de proportionnalité.

4.1.1.2. Exemptions concernant la sécurité nationale pour les autorités répressives

74. L'article 88 de la DUAA met à jour les exemptions concernant la sécurité nationale existantes dans le cadre répressif afin de refléter celles prévues par le RGPD britannique et les régimes des services de renseignement ⁽⁵¹⁾. Bien que les autorités répressives soient déjà en mesure de limiter certaines obligations pour des raisons de protection de la sécurité nationale — telles que

⁽⁴⁹⁾ La Commission souligne que, comme décrit aux considérants 139 à 141 de la décision d'exécution (UE) 2021/1772, des autorités répressives spécifiques peuvent également exercer des pouvoirs d'enquête ciblés au titre de l'IPA 2016 aux fins de la prévention ou de la détection d'infractions graves. Les modifications apportées à ces dispositions concernent donc non seulement l'accès aux données à des fins de sécurité nationale, mais aussi à des fins répressives.

⁽⁵⁰⁾ Article 261, paragraphe 10, point c), de l'IPA 2016, tel qu'inséré par l'article 19 de la loi modificative de 2024 sur les pouvoirs d'enquête.

⁽⁵¹⁾ Voir également la publication du ministère des Sciences, de l'Innovation et de la Technologie, *Data (Use and Access) Act factsheet: UK GDPR and DPA* (fiche d'information sur la DUAA: RGPD britannique et DPA), publiée le 27 juin 2025, p. 14 <https://www.gov.uk/government/publications/data-use-and-access-act-2025-factsheets/data-use-and-access-act-factsheet-uk-gdpr-and-dpa>.

celles relatives aux droits des personnes concernées — l'article 78A de la DPA 2018 inclura ⁽⁵²⁾ également la majorité des principes de protection des données⁽⁵³⁾ et certaines exigences internationales en matière de transfert de données⁽⁵⁴⁾ parmi les dispositions auxquelles il est possible de déroger si cela est nécessaire aux fins de la protection de la sécurité nationale. En outre, certains des pouvoirs dont dispose l'ICO pour effectuer des inspections et prendre des mesures répressives ⁽⁵⁵⁾ peuvent ne pas s'appliquer dans de telles circonstances.

75. Ces modifications ne sont mentionnées ni dans le projet de décision d'adéquation au titre de l'article 45 du RGPD ni dans le projet de décision d'adéquation au titre de l'article 36 de la directive en matière de protection des données dans le domaine répressif. Toutefois, le comité estime qu'il est essentiel d'évaluer ces exemptions étendues au regard des principes de nécessité et de proportionnalité. Dans ce contexte, le comité rappelle la deuxième des quatre «garanties essentielles européennes»: toute limitation de l'exercice des droits et libertés reconnus par la Charte doit respecter leur contenu essentiel et, dans le respect du principe de proportionnalité, ne peut être apportée que si elle est nécessaire et répond effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui ⁽⁵⁶⁾. Le comité fait part de son inquiétude quant à ces exemptions concernant des principes fondamentaux de la protection des données, des exigences en matière de transferts internationaux et des pouvoirs de l'ICO.
76. En vertu de la règle révisée, cinq des six principes de protection des données peuvent être écartés lorsque cela est nécessaire pour protéger la sécurité nationale ⁽⁵⁷⁾. Ces principes disposent, entre autres, que la finalité répressive pour laquelle les données à caractère personnel sont collectées doit être précisée, explicite et légitime, et que les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard de cette finalité. Ils précisent également que les données à caractère personnel doivent être exactes et conservées uniquement aussi longtemps que nécessaire. Comme indiqué ci-dessus, les futures exemptions couvrent en outre certaines des exigences en matière de transfert international, telles que la «deuxième condition pour les transferts internationaux» énoncée à l'article 73, paragraphe 3, de la DPA 2018. Cette condition exige que les transferts soient fondés soit sur des règlements d'adéquation, soit sur des garanties appropriées, soit, en l'absence de tels règlements ou garanties, sur des circonstances particulières. Les exemptions ont

⁽⁵²⁾ La DUAA sera mise en place progressivement, en plusieurs étapes. Les principales modifications apportées à la législation sur la protection des données dans la partie 5 de la DUAA prendront effet dans le cadre de l'étape 3, environ 6 mois après la sanction royale, <https://www.gov.uk/guidance/data-use-and-access-act-2025-plans-for-commencement>.

⁽⁵³⁾ Voir l'article 78A paragraphe 1, paragraphe 2, point a et paragraphe 3, de la DPA 2018, tel qu'introduit par l'article 88 de la DUAA.

⁽⁵⁴⁾ Voir l'article 78A, paragraphe 1, paragraphe 2, point d et paragraphe 4, de la DPA 2018, tel qu'introduit par l'article 88 de la DUAA.

⁽⁵⁵⁾ Voir l'article 78A, paragraphe 1, paragraphe 2, points e, f, g, de la DPA 2018, tel qu'introduit par l'article 88 de la DUAA.

⁽⁵⁶⁾ Voir les recommandations 02/2020 du comité sur les garanties essentielles européennes pour les mesures de surveillance, adoptées le 10 novembre 2020, page 10.

⁽⁵⁷⁾ Conformément à l'article 78A, paragraphes 2 et 3, de la DPA 2018, le chapitre 2 de la partie 3 de cette loi ne s'applique pas si cela est nécessaire aux fins de la protection de la sécurité nationale, à l'exception a) de l'article 35, paragraphe 1 (le premier principe en matière de protection des données) dans la mesure où il exige que le traitement de données à caractère personnel soit licite; b) de l'article 35, paragraphes 2 à 5 (licéité du traitement et restrictions sur le traitement de données sensibles); c) de l'article 42 (garanties: traitement de données sensibles); et d) de l'annexe 8 (conditions du traitement de données sensibles).

également une incidence sur les pouvoirs de l'IC, par exemple le pouvoir de publier des avis d'information et d'exécution ⁽⁵⁸⁾.

77. Le comité constate que, bien que les exemptions s'écartent clairement de la directive en matière de protection des données dans le domaine répressif, elles sont très similaires aux exceptions et restrictions en matière de sécurité nationale prévues à l'article 11 de la convention 108 modernisée du Conseil de l'Europe («convention 108+») ⁽⁵⁹⁾, que le Royaume-Uni a signée le 10 octobre 2018 mais qui, à la date du présent avis, n'a pas encore été ratifiée par le Royaume-Uni ou n'est pas encore entrée en vigueur ⁽⁶⁰⁾. À cet égard, le comité rappelle que le comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel a récemment publié des lignes directrices sur les principes généraux de l'article 11 de la convention modernisée 108 ⁽⁶¹⁾.
78. Dans ses lignes directrices, le Conseil de l'Europe souligne explicitement qu'aucune exception n'est applicable, entre autres, aux principes de proportionnalité et de légitimité de la finalité poursuivie par le traitement. Cela implique que la proportionnalité du traitement des données doit être garantie, tout comme les exigences relatives au traitement des données à caractère personnel à des fins légitimes. Conformément aux orientations du comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, le comité reste particulièrement vigilant en ce qui concerne toute exemption au principe de proportionnalité, ainsi qu'à l'obligation de traiter des données à caractère personnel à des fins légitimes. De même, selon le comité, toute exemption aux pouvoirs de l'autorité de contrôle devrait être abordée avec prudence. Bien que des exigences spécifiques applicables aux activités de contrôle – telles que les habilitations de sécurité – puissent être appropriées dans le cadre du traitement lié à la sécurité nationale, il est essentiel d'assurer un contrôle efficace pour éviter la création d'un vide prudentiel. Dans le même esprit, l'article 11, paragraphe 3, de la Convention 108+ prévoit que les exemptions à l'article 15 ⁽⁶²⁾ sont «sans préjudice de l'exigence que les activités de traitement à des fins de sécurité nationale et de défense fassent l'objet d'un contrôle et d'une supervision indépendants effectifs selon la législation nationale» des parties à la Convention. En outre, toute exemption devrait être interprétée de la manière la plus restrictive possible. Le fait que des données à caractère personnel soient traitées à des fins de sécurité nationale ne devrait pas suffire à lui seul pour qu'une exemption puisse être invoquée. Il convient de préciser qu'une exemption au régime de protection des données doit être appliquée au cas par cas et uniquement si cela est nécessaire et proportionné ⁽⁶³⁾.

⁽⁵⁸⁾ Les avis d'information exigent d'un responsable du traitement ou d'un sous-traitant qu'ils fournissent au *Commissioner* les informations raisonnablement nécessaires à l'exercice de ses fonctions. Les avis d'exécution habilitent le *Commissioner* à exiger d'une personne qu'elle prenne (ou s'abstienne de prendre) des mesures spécifiques, et ce lorsque le *Commissioner* est convaincu que la personne ne respecte pas certaines obligations en matière de protection des données.

⁽⁵⁹⁾ Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (CETS n° 223).

⁽⁶⁰⁾ <https://www.coe.int/en-GB/web/conventions/full-list?module=signatures-by-treaty&treatynum=223>

⁽⁶¹⁾ <https://rm.coe.int/t-pd-2021-7rev13-interpretation-of-general-principles-article-11-c108-/1680b6c146>

⁽⁶²⁾ Voir l'article 15 de la Convention 108+ qui précise comment les parties à la Convention, en prévoyant une ou plusieurs autorités de contrôle, doivent veiller au respect des dispositions de la Convention.

⁽⁶³⁾ Voir également l'article 11 de la Convention 108+, qui précise que les exceptions doivent être prévues par la loi, respecter l'essence des droits et libertés fondamentales et constituer une mesure nécessaire et proportionnée dans une société démocratique. Selon les lignes directrices du comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel sur les principes généraux prévus à l'article 11, cela suppose qu'une mise en balance des intérêts en présence entre la nécessité de prévoir des exceptions

79. Étant donné que les projets de décisions d'adéquation n'abordent pas ce point, le comité invite la Commission à compléter son évaluation dans le projet de décision et à suivre spécifiquement l'application dans la pratique des exemptions concernant la sécurité nationale pour les autorités répressives.

4.1.2. Responsabilité conjointe du traitement entre les services de renseignement et les autorités répressives du Royaume-Uni

80. Sur la base des modifications apportées par la DUAA, les activités de traitement menées par les autorités répressives compétentes peuvent, dans certaines circonstances spécifiques, relever des règles normalement applicables au traitement des données à caractère personnel par les autorités nationales de sécurité ⁽⁶⁴⁾. En d'autres termes, sous réserve des conditions énoncées à l'article 89 de la DUAA, le régime de protection des données pour le traitement des données relatives à la sécurité nationale établi dans la partie 4 de la DPA 2018 est étendu au traitement des données par les autorités répressives.
81. La Commission souligne que les conditions prévues à l'article 89 de la DUAA prévoient des garanties strictes: une autorité compétente doit être nommée en tant qu'«autorité compétente qualifiée» dans les règlements adoptés par le secrétaire d'État, lequel doit en outre désigner une activité de traitement particulière exercée par l'autorité compétente qualifiée en tant que responsable conjoint du traitement avec au moins un service de renseignement aux fins de la protection de la sécurité nationale ⁽⁶⁵⁾.
82. Tout en reconnaissant que ces garanties entraînent des restrictions importantes, le comité invite la Commission à suivre la mise en œuvre pratique de ces règles. Il convient de veiller tout particulièrement à ce que la partie 4 de la DPA 2018 soit appliquée strictement aux opérations de traitement à des fins de sécurité nationale, sans être étendue à d'autres contextes. Bien que les États disposent d'une large marge d'appréciation en matière de sécurité nationale, ainsi que l'a également reconnu la Cour européenne des droits de l'homme ⁽⁶⁶⁾, le comité estime qu'il convient d'opérer une distinction parmi les menaces pour la sécurité nationale sur le fondement de leur nature, de leur gravité et des circonstances spécifiques découlant de risques généraux pour la sécurité publique ou d'infractions pénales graves. Ce n'est que dans ces cas que l'action des autorités répressives dans le cadre du régime de protection des données des services de renseignement est compatible avec les principes de nécessité et de proportionnalité ⁽⁶⁷⁾. En outre, le comité estime qu'il est nécessaire de suivre si les autorités compétentes sont en mesure, dans la pratique, de maintenir une distinction claire entre les différentes finalités du traitement afin de respecter le cadre juridique correspondant en conséquence.

à certaines dispositions de la convention et le respect des droits de l'homme et des libertés fondamentales des personnes physiques doit être effectuée et motivée.

⁽⁶⁴⁾ Voir le considérant 72 du projet de décision.

⁽⁶⁵⁾ Voir le considérant 73 du projet de décision.

⁽⁶⁶⁾ Voir *CouEDH, Big Brother Watch et autres c. Royaume-Uni*, 25 mai 2021, paragraphe 350.

⁽⁶⁷⁾ Il ressort de la jurisprudence de la CJUE, lors de l'application du critère de la nécessité et de la proportionnalité à la législation des États membres autorisant l'accès des autorités publiques aux données à caractère personnel et la conservation de celles-ci par ces mêmes autorités, que les objectifs légitimes, tels que la sécurité nationale ou la lutte contre les formes graves de criminalité, présentent des différences et pourraient donc justifier des types d'atteinte différents. Voir CJUE, affaires jointes C-511/18, C-512/18 et C-520/18, *La Quadrature du Net e.a.*, 6 octobre 2020.

4.1.3. Droit d'accès

83. La DUAA précise que les personnes concernées n'ont le droit d'accéder aux informations pertinentes que dans la mesure où le responsable du traitement est en mesure de fournir celles-ci sur la base d'une recherche raisonnable et proportionnée. Cette modification est introduite à la fois dans le régime d'application de la loi et dans celui relatif à la sécurité nationale ⁽⁶⁸⁾.
84. La Commission explique qu'il s'agit d'une clarification conforme aux normes établies dans la jurisprudence nationale, lesquelles tiennent également compte des intérêts de la personne concernée. Néanmoins, le comité aurait apprécié des informations plus détaillées sur la manière dont la notion de «recherche raisonnable et proportionnée» est interprétée, d'autant plus qu'un tel élément est absent de l'article 14 de la directive en matière de protection des données dans le domaine répressif. Le comité reconnaît qu'il peut effectivement exister des circonstances dans lesquels les efforts déployés par un responsable du traitement pour identifier et localiser des informations concernant la personne concernée pourraient être considérés comme déraisonnables et disproportionnés sans pour autant compromettre l'équivalence essentielle ⁽⁶⁹⁾. Le comité rappelle l'analyse et la conclusion figurant au paragraphe 34 du présent avis, qui sont tout aussi pertinentes pour le régime d'application de la loi que pour celui relatif à la sécurité nationale.

4.1.4. Transferts ultérieurs

4.1.4.1. Un nouveau critère de protection des données

85. Lorsqu'une autorité compétente a l'intention de partager des données à caractère personnel traitées en vertu de la partie 3 de la DPA 2018 avec les autorités répressives d'un pays tiers, des exigences spécifiques s'appliquent. En particulier, ces transferts peuvent avoir lieu lorsqu'ils sont approuvés dans les règlements adoptés par le secrétaire d'État ou, en l'absence de tels règlements, sur la base de garanties appropriées. Si un transfert ne peut être fondé ni sur un règlement ni sur des garanties appropriées, il ne peut avoir lieu que dans certaines circonstances déterminées, appelées «circonstances particulières» et correspondant aux situations et conditions pouvant être qualifiées de «dérogations» au titre de l'article 38 de la directive en matière de protection des données dans le domaine répressif.
86. Bien que la Commission observe que «le régime applicable aux transferts internationaux de données à caractère personnel en provenance du Royaume-Uni reste très proche des règles énoncées au chapitre V de la directive (UE) 2016/680», le projet de décision indique également que la norme juridique applicable aux règlements relatifs à l'approbation des transferts, qualifiés de règlements d'adéquation dans l'ancien article 74A de la DPA 2018, ainsi que les garanties appropriées, ont été reformulées. Au lieu de faire référence à un niveau de protection adéquat, le nouveau «critère de protection des données» énoncé à l'article 74AB de la DPA 2028 exige que le niveau de protection des personnes concernées dans les pays tiers ou les organisations internationales destinataires ne soit «pas sensiblement inférieur» au niveau prévu pour les personnes concernées par la législation britannique pertinente en matière de protection des données.

⁽⁶⁸⁾ Voir l'article 78, paragraphes 3 et 4, de la DUAA, modifiant les articles 45 et 94 de la DPA 2018.

⁽⁶⁹⁾ Par exemple, on pourrait faire valoir que tel est le cas pour la recherche de dispositifs saisis qui n'ont pas encore été analysés ou déchiffrés.

87. Dans ce contexte, le comité note que les éléments que le secrétaire d'État doit prendre en considération dans l'évaluation au titre de l'article 74AB, paragraphe 2, de la DPA 2018 semblent avoir été réduits par rapport à l'évaluation précédente des règlements relatifs à l'adéquation ⁽⁷⁰⁾. Le comité souligne la suppression de certains facteurs qui, selon lui, jouent un rôle important dans l'évaluation de la question de savoir si un pays tiers offre un niveau de protection des données à caractère personnel essentiellement équivalent et rappelle l'analyse et les conclusions formulées aux paragraphes 42 et 43 du présent avis. En particulier, le comité i) encourage la Commission à examiner spécifiquement les changements et à approfondir son évaluation du nouveau critère de protection des données. Le comité comprend que les nouvelles règles relatives aux transferts de données à caractère personnel vers des pays tiers visent à offrir une flexibilité supplémentaire. Dans le même temps, le comité invite la Commission à suivre l'application pratique de ces règles dans le domaine de la coopération en matière répressive et de justice pénale. Un tel suivi est particulièrement pertinent en ce qui concerne le nouveau pouvoir du secrétaire d'État d'adopter des règlements qui identifient et approuvent un transfert sur la base du nouveau critère en matière de protection des données, et ce par tout moyen, y compris en se référant aux secteurs géographiques d'un pays, aux responsables du traitement ou aux sous-traitants, aux destinataires des données, aux types de données, aux moyens de transfert et aux instruments juridiques. Il reste difficile de savoir, par exemple, comment un responsable du traitement ou un sous-traitant spécifique établi dans un pays tiers qui n'est pas considéré comme adéquat satisferait au critère en matière de protection des données en ce qui concerne des mécanismes de recours effectifs ou les droits des personnes concernées qui ne sont pas déjà inscrits dans le cadre juridique de ce pays tiers.
88. En outre, le comité rappelle les conclusions exposées au paragraphe 41 en ce qui concerne l'utilisation du critère de l'«opportunité de faciliter les transferts de données à caractère personnel à destination et en provenance du Royaume-Uni» [article 74 AA, paragraphe 3, de la DPA 2018) et invite la Commission à préciser dans sa décision que ce critère n'est pas un élément du critère relatif à la protection des données, mais simplement un facteur supplémentaire que le secrétaire d'État peut examiner lorsque les exigences liées au critère sont pleinement remplis, étant donné que cela ne ressort pas de façon parfaitement claire du texte de la loi. À cet égard, le comité invite la Commission à suivre les implications pratiques de l'article 74AA, paragraphe 3, de la DPA 2018, étant donné qu'il reste à voir quel rôle jouera, dans ce contexte, l'«opportunité de faciliter les transferts de données à caractère personnel à destination et en provenance du Royaume-Uni».

4.1.4.2. Accord au titre de la loi américaine sur l'informatique en nuage (Cloud Act) conclu entre le Royaume-Uni et les États-Unis

89. Une autre évolution pertinente dans le domaine des transferts ultérieurs est l'entrée en vigueur, en octobre 2022, de 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 à des fins de lutte contre la grande criminalité» (l'accord au titre de la loi américaine sur l'informatique en nuage (Cloud Act) conclu entre le Royaume-Uni et les États-Unis»). Comme la Commission le souligne à juste titre, les données à caractère personnel transférées de l'UE vers des fournisseurs de services au Royaume-Uni pourraient faire l'objet

⁽⁷⁰⁾ La disposition de l'article 74A, paragraphe 4, de la DPA 2018, qui n'a pas été reprise dans la DUAA, prévoyait une liste de critères identiques à ceux figurant à l'article 36, paragraphe 3, de la directive en matière de protection des données dans le domaine répressif.

d'injonctions de production de preuves émises par des autorités répressives américaines compétentes en vertu de cet accord ⁽⁷¹⁾.

90. Étant donné qu'au moment de l'adoption de la précédente décision d'adéquation concernant le Royaume-Uni, l'accord avait été conclu mais n'était pas encore entré en vigueur, la Commission a souligné que toute information et toute clarification future concernant la manière dont les États-Unis se conformeront aux obligations qui leur incombent en vertu de l'accord devraient être communiquées par le Royaume-Uni à la Commission, afin de garantir un suivi approprié de la précédente décision d'adéquation concernant le Royaume-Uni, conformément à l'article 45, paragraphe 4, du RGPD. La Commission a constaté qu'une attention particulière devrait être accordée à l'application et à l'adaptation des garanties établies dans l'accord-cadre UE-États-Unis ⁽⁷²⁾ au type spécifique de transferts couverts par l'accord au titre de la loi américaine sur l'informatique en nuage (Cloud Act) conclu entre le Royaume-Uni et les États-Unis ⁽⁷³⁾. Dans le prolongement de cette déclaration, la Commission fait référence dans son projet de décision à plusieurs clarifications convenues entre le Royaume-Uni et les États-Unis lors l'application de l'accord-cadre UE-États-Unis à l'accord au titre de la loi américaine sur l'informatique en nuage (Cloud Act) conclu entre le Royaume-Uni et les États-Unis. Le comité salue ces précisions, qui apportent davantage de clarté juridique. Parallèlement, il convient de noter que l'accord-cadre entre l'UE et les États-Unis n'a pas encore été réexaminé, ce qui limite dans une certaine mesure les conclusions qui peuvent être tirées sur l'incidence et l'efficacité de son application à l'accord au titre de la loi américaine sur l'informatique en nuage (Cloud Act) conclu entre le Royaume-Uni et les États-Unis ⁽⁷⁴⁾. En outre, eu égard à l'accord-cadre UE-États-Unis, le comité souhaite rappeler la nécessité d'améliorer le niveau de garanties prévu par cet accord. Cela s'applique en particulier à l'existence de recours juridictionnel. Les personnes concernées de l'UE qui ne sont pas citoyens de l'UE ne disposent d'aucun fondement juridique en vertu de la *Judicial Redress Act* (loi sur le recours juridictionnel) pour exercer des voies de recours. En outre, la *Privacy Act* (loi sur la protection de la vie privée) contient des exceptions, qui n'ont pas été modifiées par la *Judicial Redress Act*, qui réduisent la capacité des personnes physiques à demander réparation dans certaines situations liées à l'application de la loi et à la sécurité nationale. Si la Commission note que la loi sur le recours juridictionnel n'est pas le seul mécanisme permettant d'exercer une voie de recours, le projet de décision se borne à indiquer que «selon les circonstances et le contexte de chaque affaire, d'autres lois américaines applicables offrent d'autres voies permettant d'exercer des voies de recours» ⁽⁷⁵⁾. La question de savoir si toutes les personnes physiques de l'UE dont les données pourraient être soumises à l'accord au titre de la loi américaine sur l'informatique en nuage (Cloud Act) conclu entre le Royaume-Uni et les États-Unis pourront exercer des voies de recours aux États-Unis n'est pas tranchée.

⁽⁷¹⁾ Voir le considérant 87 du projet de décision.

⁽⁷²⁾ 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, JO L 336 du 10.12.2016, p. 3–13, [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22016A1210\(01\)](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22016A1210(01)).

⁽⁷³⁾ Voir considérant 155 de la décision d'exécution 2021/1772. Conformément à l'article 9, paragraphe 1 de l'accord au titre de la loi américaine sur l'informatique en nuage (Cloud Act) conclu entre le Royaume-Uni et les États-Unis, l'accord-cadre entre l'Union européenne et les États-Unis s'applique *mutatis mutandis* à l'accord au titre de la loi américaine sur l'informatique en nuage (Cloud Act) conclu entre le Royaume-Uni et les États-Unis. Il ne peut s'appliquer que *mutatis mutandis*, étant donné que l'accord-cadre régit les transferts transfrontières entre les services répressifs, et non la coopération directe entre un prestataire de services et une autorité répressive.

⁽⁷⁴⁾ Voir l'article 23 de l'accord-cadre UE-États-Unis, qui prévoit que les parties procèdent à des examens périodiques conjoints des politiques et des procédures mettant en œuvre l'accord, le premier examen étant réalisé au plus tard trois ans après la date d'entrée en vigueur de l'accord. L'accord-cadre entre l'UE et les États-Unis est entré en vigueur en février 2017.

⁽⁷⁵⁾ Voir le considérant 93 du projet de décision.

91. Le comité note également qu'une garantie réciproque spécifique prévue dans l'accord au titre de la loi américaine sur l'informatique en nuage (Cloud Act) conclu entre le Royaume-Uni et les États-Unis, en vertu de laquelle les deux parties limitent l'incidence que l'accord peut avoir, respectivement, sur les ressortissants britanniques et américains, n'est, par nature, pas applicable aux personnes physiques de l'UE ⁽⁷⁶⁾. Le comité observe que, pour cette raison, des garanties solides en matière de protection des données sont essentielles pour assurer la protection adéquate des droits des personnes concernées de l'UE lorsque leurs données sont traitées dans le cadre de cet accord. Par conséquent, le comité invite la Commission à continuer à prendre en considération l'accord au titre de la loi américaine sur l'informatique en nuage (Cloud Act) conclu entre le Royaume-Uni et les États-Unis dans ses futures évaluations et examens de la décision d'adéquation.
92. Dans l'ensemble, le comité estime qu'il est nécessaire d'apporter des clarifications concernant l'évaluation par la Commission de l'accord au titre de la loi américaine sur l'informatique en nuage (Cloud Act) conclu entre le Royaume-Uni et les États-Unis et toute incidence éventuelle de l'accord sur le niveau de protection, tel qu'évalué dans la précédente décision d'adéquation concernant le Royaume-Uni. Les conclusions du premier examen de l'accord au titre de la loi américaine sur l'informatique en nuage (Cloud Act) conclu entre le Royaume-Uni et les États-Unis, qui, en vertu de l'article 12, paragraphe 1, de l'accord, doit être effectué dans un délai d'un an à compter de l'entrée en vigueur de l'accord, pourraient être particulièrement instructives pour une telle analyse approfondie.

4.1.5. Contrôle et voies de recours

93. Le comité note que le système de contrôle des autorités chargées de l'application du droit pénal en vertu de la DPA 2018 et de l'IPA 2016, ainsi que les mécanismes de recours prévus à la partie 3 de la DPA 2018, de l'IPA 2016 et de la *Human Rights Act 1998* (loi de 1998 sur les droits de l'homme), restent largement inchangés. En particulier, le contrôle au Royaume-Uni continue d'être assuré, outre l'ICO, par une combinaison de différents commissaires, à savoir l'*Investigatory Powers Commissioner* (commissaire aux pouvoirs d'enquête, IPC), assisté par d'autres commissaires judiciaires, ainsi que le *Biometrics and Surveillance Camera Commissioner* (commissaire à la biométrie et aux caméras de surveillance).
94. Comme la Commission l'a expliqué au considérant 97 du projet de décision, la loi modificative de 2024 sur les pouvoirs d'enquête n'a apporté que des modifications limitées, notamment par l'introduction d'IPC adjoints auxquels l'IPC peut déléguer des pouvoirs spécifiques lorsqu'il n'est pas en mesure d'exercer ses fonctions ou n'est pas disponible à cette fin. Ces IPC adjoints doivent être des commissaires judiciaires et sont nommés par l'IPC.
95. Le comité note avec satisfaction que les idées précédentes contenues dans le projet de loi sur la protection des données et les informations numériques, qui a précédé la DUUA, visant à supprimer le poste de commissaire à la biométrie et aux caméras de surveillance et à transférer ses fonctions à l'IPC, ont été abandonnées ⁽⁷⁷⁾. À cet égard, le comité invite la Commission à accorder une attention accrue et à fournir une évaluation plus détaillée du rôle du commissaire

⁽⁷⁶⁾ Voir l'article 4, paragraphe 3 et l'article 7, paragraphe 1, de l'accord, qui prévoient des restrictions ciblées, en vertu desquelles les injonctions faisant l'objet de l'accord ne peuvent pas cibler intentionnellement une «personne se trouvant dans la partie destinataire». Par conséquent, les États-Unis ne peuvent pas cibler intentionnellement une personne se trouvant sur le territoire du Royaume-Uni, et le Royaume-Uni doit se conformer à une restriction similaire.

⁽⁷⁷⁾ Voir <https://www.gov.uk/government/organisations/biometrics-and-surveillance-camera-commissioner>.

à la biométrie et aux caméras de surveillance dans le système de contrôle au cours de son suivi et de ses futurs examens du projet de décision.

96. Comme l'a déjà souligné le comité dans son avis 14/2021, bien que l'ICO soit dotée des pouvoirs nécessaires, qui correspondent étroitement à ceux des autorités de contrôle des États membres de l'UE tels que définis à l'article 58 du RGPD, l'existence de sanctions effectives joue un rôle important s'agissant de garantir le respect des règles ⁽⁷⁸⁾.
97. Le comité prend note avec satisfaction de la politique de transparence de l'ICO et de la disponibilité des données statistiques et analytiques, y compris des exemples, concernant les activités répressives de l'ICO vis-à-vis des services répressifs ⁽⁷⁹⁾. À cet égard, le comité constate que l'autorité britannique de contrôle préfère prononcer des réprimandes en cas de violation de la législation sur la protection des données par l'intermédiaire des forces de police. L'avis d'exécution adressé au ministère public en janvier 2024 constitue une exception notable ⁽⁸⁰⁾. Le comité considère également comme positif le fait que l'ICO ait publié de nombreux codes de bonnes pratiques, lignes directrices, avis et autres documents d'orientation à l'intention des parties concernées.
98. À la lumière de ce qui précède, et en particulier compte tenu des changements substantiels imminents dans la structure et l'organisation de l'autorité de contrôle britannique, comme déjà analysé au paragraphe 68 du présent avis, le comité invite la Commission européenne à continuer de surveiller l'efficacité des sanctions et des voies de recours pertinentes dans le cadre de protection des données du Royaume-Uni.

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

99. Le projet de décision ne fournit que peu de détails sur l'accès aux données à caractère personnel et leur utilisation par les autorités publiques britanniques à des fins de sécurité nationale. La Commission explique que la DUAA n'a apporté que des modifications mineures au cadre régissant le traitement des données par les services de renseignement britanniques ⁽⁸¹⁾, dont certaines ont également été introduites dans le régime répressif de la DPA 2018. Ces modifications sont brièvement mentionnées au considérant 75 du projet de décision. En outre, les modifications apportées à l'IPA 2016 depuis l'adoption de la précédente décision d'adéquation concernant le Royaume-Uni sont déjà abordées à la section 3.2 du projet de décision, où elles concernent à la fois le traitement des données à des fins répressives et à des fins de sécurité nationale ⁽⁸²⁾. En conséquence, les demandes de clarification et de suivi décrites aux sections 4.1.1.1 et 4.1.3 ci-dessus s'appliquent également à l'accès et à l'utilisation des données à caractère personnel à des fins de sécurité nationale.

4.2.1. Utilisation des avis sur les capacités techniques

100. Au début de l'année, les médias ont révélé que le gouvernement britannique aurait émis un avis sur les capacités techniques en vertu de l'article 253 de l'IPA 2016 à l'encontre d'une grande

⁽⁷⁸⁾ Voir avis 14/2021 du comité européen de la protection des données, paragraphe 112.

⁽⁷⁹⁾ Voir, par exemple, les ensembles de données détaillés sur les réclamations en matière de protection des données disponibles à l'adresse suivante: <https://ico.org.uk/action-weve-taken/complaints-and-concerns-data-sets/data-protection-complaints/>.

⁽⁸⁰⁾ Voir <https://ico.org.uk/action-weve-taken/enforcement/crown-prosecution-service-1/>.

⁽⁸¹⁾ Voir le considérant 75 du projet de décision.

⁽⁸²⁾ Voir le considérant 98 du projet de décision. Les pouvoirs d'enquête en question peuvent être exercés non seulement par les agences nationales de renseignement, mais aussi par certaines autorités répressives.

entreprise technologique, exigeant que le fournisseur soit en mesure de conserver l'accès aux données cryptées de ses utilisateurs sous forme décryptée ⁽⁸³⁾. Dans la pratique, cela signifierait prétendument de contourner le chiffrement de bout en bout que le fournisseur propose pour sa solution de stockage en nuage. Cette mesure a donc été qualifiée de «demande détournée».

101. Bien que la base juridique des avis sur les capacités techniques existait déjà au moment de l'adoption de la précédente décision d'adéquation concernant le Royaume-Uni, le cas signalé semble constituer le premier exemple connu d'une application de ce type. En tant que telle, il s'agit d'une évolution importante qui mérite une attention particulière, en particulier à la lumière de l'article 45, paragraphe 2, point a), du RGPD, qui exige une évaluation du cadre juridique non seulement sur le papier, mais aussi de sa mise en œuvre ⁽⁸⁴⁾. Le comité se serait donc attendu à ce que le projet de décision traite explicitement cette question et encourage la Commission à compléter la décision en conséquence.
102. Bien que les détails de cette affaire ne soient pas pleinement connus du public en raison de la nature confidentielle des avis sur les capacités techniques, il ressort de l'avis public concernant la demande de huis clos figurant sur le site web du tribunal chargé des pouvoirs d'enquête, ainsi que de l'extrait accessible au public de la décision rendue à huis clos dans le cadre de cette audience, qu'il ne s'agit pas de spéculations médiatiques ⁽⁸⁵⁾. La question mérite d'être mentionnée et l'application alléguée de l'article 253 de l'IPA 2016 pour émettre une «demande détournée» devrait être signalée en vue d'un suivi futur.
103. Comme récemment souligné dans la déclaration 5/2024, le comité considère que le chiffrement est essentiel pour garantir la sécurité et la confidentialité des données à caractère personnel et des communications électroniques. En particulier, un véritable chiffrement de bout en bout couvrant les terminaux et les données qu'ils contiennent, dont les clés de déchiffrement sont détenues exclusivement par l'utilisateur, est un outil essentiel pour garantir la confidentialité des communications électroniques ⁽⁸⁶⁾. Les avis sur les capacités techniques qui obligent les entreprises à fournir la possibilité de supprimer le cryptage à la demande du gouvernement créent des vulnérabilités systémiques et constituent une menace directe pour l'intégrité et la confidentialité des communications électroniques. À cet égard, le comité attire l'attention sur l'affaire *PODCHASOV c. RUSSIE*, dans laquelle la Cour européenne des droits de l'homme a estimé que «l'obligation de décrypter les communications cryptées de bout en bout risque d'équivaloir à une exigence imposée aux fournisseurs de ces services d'affaiblir le mécanisme de cryptage pour tous les utilisateurs; elle n'est donc pas proportionnée par rapport aux objectifs légitimes poursuivis» ⁽⁸⁷⁾.
104. Bien qu'il soit supposé que le gouvernement britannique chercherait principalement à accéder aux données non cryptées des utilisateurs s'il existait un risque pour la sécurité nationale, le comité considère que la demande d'évaluation de l'utilisation des avis sur les capacités

⁽⁸³⁾ Cf. «U.K. orders Apple to let it spy on users' encrypted accounts» (Le Royaume-Uni ordonne à Apple de lui permettre d'espionner les comptes cryptés des utilisateurs, Washington Post, 7 février 2025).

<https://www.washingtonpost.com/technology/2025/02/07/apple-encryption-backdoor-uk/>.

⁽⁸⁴⁾ En outre, l'article 45, paragraphe 3, du RGPD précise que la Commission prend en compte toutes les évolutions pertinentes dans le pays tiers lorsqu'elle examine périodiquement leurs constatations d'adéquation.

⁽⁸⁵⁾ Voir <https://www.judiciary.uk/judgments/apple-inc-v-secretary-of-state-for-the-home-department/>.

⁽⁸⁶⁾ Voir la déclaration 5/2024 sur les recommandations du groupe de haut niveau concernant l'accès aux données pour une application efficace des lois, adoptée le 4 novembre 2024, p. 4 et 5.

⁽⁸⁷⁾ Voir arrêt de la CouEDH du 13 février 2024, 33696/19, paragraphe 79.

techniques, telle qu'examinée ci-dessus, est tout aussi pertinente dans le contexte de l'accès des pouvoirs publics à des fins répressives.

4.2.2. Bases juridiques et garanties applicables

105. La loi modificative de 2024 sur les pouvoirs d'enquête a introduit un régime spécifique pour la conservation et l'examen d'ensembles de données à caractère personnel en masse pour lesquels les personnes physiques auxquelles les données à caractère personnel se rapportent «ne peuvent avoir aucune attente raisonnable en matière de confidentialité, ou seulement une attente raisonnable très limitée», comme le prévoit la loi ⁽⁸⁸⁾. Pour la conservation et l'examen de ce sous-ensemble spécifique d'ensembles de données à caractère personnel en masse, l'IPA 2016 prévoit désormais la possibilité d'«autorisations individuelles» et d'«autorisations par catégorie». ⁸⁹
106. La notion d'ensembles de données à caractère personnel en masse est large et peut englober un large éventail d'ensembles de données ⁽⁹⁰⁾. Cela peut s'appliquer aux informations sensibles, mais peut également concerner les données accessibles au public et disponibles dans le commerce. Dans ce contexte, le gouvernement britannique a jugé nécessaire de réviser le régime précédent qui appliquait le même niveau de garanties à tous les ensembles de données à caractère personnel en masse et de prévoir, au lieu de cela, des garanties différentes en ce qui concerne la conservation et l'examen des ensembles de données à caractère personnel en masse, en fonction de la sensibilité ou de la disponibilité publique de leur contenu, ou du niveau d'intrusion associé aux services de renseignement qui les conservent et les examinent ⁽⁹¹⁾. Le comité croit comprendre que ces considérations ont finalement conduit à la création d'un régime distinct pour les ensembles de données à caractère personnel en masse pour lesquels il n'existe qu'une aucune attente raisonnable en matière de confidentialité, ou seulement une attente raisonnable très limitée.
107. Bien que la Commission examine brièvement la nouvelle notion d'«autorisation par catégorie», le projet de décision indique qu'«il est important de noter que, pour la conservation et l'examen d'ensembles de données à caractère personnel en masse, le régime évalué aux considérants 239 et 240 de la décision d'exécution (UE) 2021/1772 reste en vigueur, en particulier la nécessité d'un mandat approuvé d'abord par le secrétaire d'État, puis par le commissaire judiciaire, sous réserve des exigences de nécessité et de proportionnalité de la mesure, comme le prévoit la

⁽⁸⁸⁾ Voir l'article 226 A, paragraphe 1, de l'IPA 2016.

⁽⁸⁹⁾ Voir les articles 226A et 226BA de l'IPA 2016, tels qu'introduits par l'article 2 de la loi modificative de 2024 sur les pouvoirs d'enquête.

⁽⁹⁰⁾ Voir l'article 199 de l'IPA 2016 qui précise qu'un «service de renseignement conserve un ensemble de données à caractère personnel si (a) le service de renseignement obtient un ensemble d'informations comprenant des données à caractère personnel relatives à un certain nombre de personnes physiques, (b) la nature de cet ensemble est telle que la majorité des personnes physiques ne présentent pas d'intérêt pour le service de renseignement dans l'exercice de ses fonctions et ne sont pas susceptibles d'en présenter à l'avenir, (c) après un premier examen du contenu, le service de renseignement conserve l'ensemble de données aux fins de l'exercice de ses fonctions, et (d) l'ensemble de données est conservé ou doit être conservé sous forme électronique à des fins d'analyse dans l'exercice de ces fonctions».

⁽⁹¹⁾ Voir Ministère de l'intérieur, *Policy paper, Investigatory Powers (Amendment) Bill: Bulk Personal Datasets and Third Party Bulk Personal Datasets* [document d'orientation, Projet de loi (modificative) sur les pouvoirs d'enquête: ensembles de données à caractère personnel en masse et ensembles de données à caractère personnel en masse de tiers], <https://www.gov.uk/government/publications/investigatory-powers-amendment-bill-factsheets/investigatory-powers-amendment-bill-bulk-personal-datasets-and-third-party-bulk-personal-datasets>.

partie 7 de l'IPA 2016»⁽⁹²⁾. Cependant, cette analyse semble incomplète. Le comité note que non seulement l'introduction d'«autorisation par catégorie», mais aussi d'«autorisation individuelles» constitue un changement pertinent mis en œuvre par la loi modificative de 2024 sur les pouvoirs d'enquête en ce qui concerne l'ensemble de données spécifique susmentionné: une «autorisation individuelle», qui peut être accordée par le chef d'un service de renseignement ou par une personne agissant en son nom, remplace la nécessité d'obtenir un mandat pour conserver ou conserver et examiner des ensembles de données à caractère personnel en masse pour lesquels il n'existe aucune attente raisonnable en matière de confidentialité, ou seulement une attente raisonnable très limitée⁽⁹³⁾. Les termes «mandat» et «autorisation individuelle» ne devraient donc pas être confondus et ne sauraient être utilisés de manière interchangeable⁽⁹⁴⁾. Cela est d'autant plus vrai que l'approbation judiciaire requise pour les autorisations individuelles se limite à déterminer si l'ensemble de données spécifique remplit les critères pour être classé dans la catégorie ne garantissant «aucune attente raisonnable en matière de confidentialité, ou seulement une attente raisonnable très limitée» au titre de l'article 226A de l'IPA 2016⁽⁹⁵⁾. Une «autorisation de catégorie» est différente d'une «autorisation individuelle» et, de fait, exclut – conformément à l'article 226B, paragraphe 6, point a), de l'IPA 2016 – l'exigence d'une telle approbation judiciaire d'une autorisation individuelle lorsque cette autorisation concerne un ensemble de données qui relève d'une autorisation de catégorie. En effet, une décision aura déjà été prise, et approuvée par un commissaire judiciaire, selon laquelle tout ensemble de données relevant de la description de l'autorisation de catégorie est effectivement un ensemble de données auquel l'article 226A s'appliquerait.

108. Bien que ces modifications concernent la conservation et l'examen d'ensembles de données à caractère personnel en masse, et non leur interception ou leur collecte initiale, le comité tient à souligner l'importance que la Cour européenne des droits de l'homme accorde à l'autorisation préalable indépendante dans le contexte du traitement de données à caractère personnel en masse. La Cour a statué qu'«afin de réduire autant que possible le risque d'abus du pouvoir d'interception en masse, [...] le processus doit être encadré par des “garanties de bout en bout”, c'est-à-dire qu'au niveau national, la nécessité et la proportionnalité des mesures prises devraient être appréciées à chaque étape du processus, que les activités d'interception en masse devraient être soumises à l'autorisation d'une autorité indépendante dès le départ – dès la définition de l'objet et de l'étendue de l'opération – et que les opérations devraient faire l'objet d'une supervision et d'un contrôle indépendant opéré a posteriori»⁽⁹⁶⁾. Dans cette optique et sur la base d'une approche holistique, tenant compte de toutes les circonstances de l'affaire pour évaluer l'adéquation, le comité considère que la conservation et l'examen de données à caractère personnel en masse devraient au moins être soumis soit à une autorisation préalable d'une autorité indépendante, soit à un examen indépendant systématique a posteriori par un tribunal ou un organisme équivalent, c'est-à-dire un organisme indépendant capable de rendre des décisions contraignantes.

⁽⁹²⁾ Voir le considérant 99 du projet de décision.

⁽⁹³⁾ Article 200, paragraphes 1 et 2, de l'IPA 2016.

⁽⁹⁴⁾ Cela semble toutefois être le cas dans les considérants 99 et 100 du projet de décision.

⁽⁹⁵⁾ L'article 226BB, paragraphe 1, de l'IPA 2016 dispose que lorsqu'il décide d'approuver ou non une décision d'octroi d'une autorisation individuelle ou d'une autorisation par catégorie, un commissaire judiciaire doit examiner les conclusions de la personne qui a accordé l'autorisation afin de vérifier si l'article 226A s'applique à l'ensemble de données à caractère personnel en masse décrit dans l'autorisation ou si l'article 226A s'applique à tout ensemble de données relevant de la catégorie des ensembles de données décrite dans l'autorisation.

⁽⁹⁶⁾ *CouEDH, Big Brother Watch et autres c. Royaume-Uni*, 25 mai 2021, paragraphe 350.

109. Compte tenu des clarifications qui restent à apporter, le comité invite instamment la Commission à examiner plus avant les concepts d'«autorisations individuelles» et d'«autorisations par catégorie» prévus par la loi modificative de 2024 sur les pouvoirs d'enquête. En outre, le comité invite la Commission à suivre de près la mise en œuvre de l'expression «aucune attente raisonnable en matière de confidentialité, ou seulement une attente raisonnable très limitée» dans la pratique. Bien que l'article 226A de l'IPA 2016 établisse un certain nombre de critères pour parvenir à une telle constatation, le comité estime qu'il est important d'observer leur application, étant donné qu'ils peuvent faire l'objet d'une interprétation large ⁽⁹⁷⁾.

4.2.3. Contrôle et voies de recours

110. Comme indiqué dans le projet de décision et analysé précédemment dans l'avis 14/2021, l'IPC et son bureau (IPCO) jouent un rôle central dans le contrôle de l'utilisation des pouvoirs d'enquête par les agences de renseignement du Royaume-Uni. En outre, le tribunal chargé des pouvoirs d'enquête est l'organe judiciaire compétent pour offrir une voie de recours à cet égard. Comme déjà indiqué à l'article 3.1.5 sur le contrôle dans le domaine répressif, la loi modificative de 2024 sur les pouvoirs d'enquête n'a apporté que des modifications limitées, notamment par l'introduction d'IPC adjoints. Par conséquent, les commentaires formulés par le comité dans son avis 14/2021 restent pleinement valables ⁽⁹⁸⁾.
111. Le comité note avec satisfaction la transparence du rapport annuel de l'IPCO, y compris la disponibilité de statistiques détaillées pour la période 2019-2023, notamment sur l'utilisation de pouvoirs de masse par la communauté du renseignement du Royaume-Uni et sur les décisions de ciblage et les autorisations ciblées aux fins de l'acquisition de données conformément à l'accord d'accès aux données entre le Royaume-Uni et les États-Unis. Le comité prend également spécifiquement note des activités de contrôle menées par l'IPCO sur l'interception en masse de données par le Centre national de communications (GCHQ), mises en évidence par la Commission au considérant 102 du projet de décision. Dans ce contexte, le comité invite la Commission à continuer de surveiller de près l'efficacité du système de contrôle dans ce domaine, en particulier en ce qui concerne la proportionnalité des demandes d'interception en masse ⁽⁹⁹⁾.
112. En outre, le comité note que le tribunal chargé des pouvoirs d'enquête a également publié un rapport public sur ses activités et sa jurisprudence pour la période 2021-2023 ⁽¹⁰⁰⁾. Le rapport met notamment en évidence des évolutions importantes et pertinentes, tels que l'arrêt rendu par la Cour européenne des droits de l'homme dans l'affaire *Wieder et Guarnieri c. Royaume-Uni*, dans lequel la Cour a statué que toute personne physique, où qu'elle se trouve dans le monde, peut introduire un recours auprès du tribunal chargé des pouvoirs d'enquête si les faits incriminés ont été commis par un organisme public britannique et se sont produits au Royaume-Uni. Le comité invite donc la Commission à inclure également les activités du tribunal chargé des pouvoirs d'enquête dans son évaluation et dans les futurs examens du projet de décision.

⁽⁹⁷⁾ L'article 226A de l'IPA 2016 fait référence, par exemple, à la nature des données, à la mesure dans laquelle les données ont été rendues publiques ou à la mesure dans laquelle elles sont largement connues.

⁽⁹⁸⁾ Voir avis 14/2021, paragraphes 200 à 215.

⁽⁹⁹⁾ Pour de plus amples informations, voir le rapport annuel 2023 du commissaire aux pouvoirs d'enquête, disponible à l'adresse suivante: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/E03270100-HC_603-IPCO-Annual-Report-2023-Web_Accessible.pdf, page 31, paragraphe 6.41.

¹⁰⁰ <https://investigatorypowerstribunal.org.uk/wp-content/uploads/2024/11/Investigatory-Powers-Tribunal-Report-2024.pdf>

5.Examen, durée et renouvellement du projet de décision

113. Le comité note que la décision d'adéquation finale s'appliquerait pendant six ans, c'est-à-dire jusqu'au 27 décembre 2031. Le Royaume-Uni resterait ainsi le seul pays tiers dont la décision d'adéquation comporte une clause de caducité combinée à l'examen périodique obligatoire prévu à l'article 45, paragraphe 3, du RGPD. Le comité comprend que le nouveau cadre juridique britannique méritera une attention particulière et invite la Commission à suivre attentivement la mise en œuvre de la DUAA, y compris les domaines prioritaires soulignés dans le présent avis, ainsi que tous les autres développements pertinents au Royaume-Uni à cet égard.
114. Le comité se félicite que le considérant 68 du projet de décision fasse référence au rôle du comité (et des groupes de la société civile) dans le mécanisme d'examen périodique, conformément à la recommandation 01/2021 du CEPD ⁽¹⁰¹⁾. En ce qui concerne l'implication pratique du comité et de ses représentants dans la préparation et le déroulement des futurs examens, le comité rappelle que toute documentation pertinente, y compris la correspondance, devra lui être communiquée par écrit suffisamment en amont des examens.
115. Sur la base des explications supplémentaires fournies par la Commission en ce qui concerne le considérant 113, le comité comprend que l'intention est de procéder à un examen à la fin des quatre années sur la base desquelles la Commission élaborera un rapport public ⁽¹⁰²⁾. Cet examen permettra à la Commission de déterminer, au plus tard six mois avant la fin du projet de décision, s'il convient d'engager la procédure visant à prolonger la durée du projet de décision ⁽¹⁰³⁾.
116. Le comité salue cette intention et note que, dans la mesure où l'examen poursuit un objectif différent de celui de la clause de caducité et joue un rôle important dans le contrôle du cadre juridique. Le comité s'attend donc à ce que l'examen ait lieu dans quatre ans et encourage la Commission à le mener à bien en temps voulu.
117. Le comité croit comprendre que ce futur examen tiendra compte des éléments décrits dans la décision d'exécution 2021/1772 de la Commission et que les considérants relatifs à la suspension et à l'abrogation de la décision sont toujours valables ⁽¹⁰⁴⁾. Dans un souci de sécurité juridique, le comité estime qu'une telle clarification pourrait figurer dans la décision d'adéquation finale.

Pour le comité européen de la protection des données

La présidente

(Anu Talus)

¹⁰¹ Voir le considérant 19 de la recommandation 01/2021 du comité européen de la protection des données.

¹⁰² Voir le considérant 110 du projet de décision.

⁽¹⁰³⁾ Voir le considérant 113 du projet de décision.

⁽¹⁰⁴⁾ Voir les considérants 168 à 171 de la décision d'exécution 2021/1173 de la Commission.