Journal officiel
de l'Union européenne

FR
Série L

2025/2574

23.12.2025

DÉCISION D'EXÉCUTION (UE) 2025/2574 DE LA COMMISSION

du 19 décembre 2025

modifiant la décision d'exécution (UE) 2021/1772 de la Commission constatant, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par le Royaume-Uni

[notifiée sous le numéro C(2025) 8771]

(Texte présentant de l'intérêt pour l'EEE)

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ([1]) (RGPD), et notamment son article 45, paragraphe 3,

considérant ce qui suit:

1. INTRODUCTION

(1) Dans la décision d'exécution (UE) 2021/1772 ([2]), la Commission conclut que, aux fins de l'article 45 du règlement (UE) 2016/679, le Royaume-Uni assure un niveau de protection adéquat des données à caractère personnel transférées dans le cadre dudit règlement de l'Union européenne vers le Royaume-Uni ([3]).

(2) Lorsqu'elle a adopté la décision d'exécution (UE) 2021/1772, la Commission a tenu compte du fait que, à l'issue de la période de transition prévue par l'accord sur le retrait du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord de l'Union européenne et de la Communauté européenne de l'énergie atomique ([4]) et dès que la disposition provisoire prévue par l'article 782 de l'accord de commerce et de coopération entre l'Union européenne et la Communauté européenne de l'énergie atomique, d'une part, et le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, d'autre part ([5]), aurait cessé de s'appliquer, le Royaume-Uni adopterait, appliquerait et mettrait en œuvre un nouveau régime de protection des données, autre que celui qui était en place lorsqu'il était lié par le droit de l'Union.

(3) Étant donné que cela pouvait donner lieu à des modifications concernant le cadre de protection des données évalué dans la décision d'exécution (UE) 2021/1772, ou à d'autres évolutions pertinentes, il a été jugé approprié de prévoir que ladite décision serait applicable pour une durée de quatre ans à compter de son entrée en vigueur. La décision d'exécution (UE) 2021/1772 devait donc expirer le 27 juin 2025, sauf si elle est prorogée conformément à la procédure visée à l'article 93, paragraphe 2, du règlement (UE) 2016/679.

([1]) JO L 119 du 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj.
([2]) Décision d'exécution (UE) 2021/1772 de la Commission du 28 juin 2021 constatant, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par le Royaume-Uni (JO L 360 du 11.10.2021, p. 1, ELI: http://data.europa.eu/eli/dec_impl/2021/1772/oj).
([3]) Voir article 1er, paragraphe 1, de la décision d'exécution (UE) 2021/1772. En vertu de l'article 1er, paragraphe 2, de ladite décision d'exécution, celle-ci ne couvre pas les données à caractère personnel transférées à des fins de contrôle de l'immigration au Royaume-Uni ou qui relèvent par ailleurs du champ d'application de l'exemption de certains droits des personnes concernées aux fins du maintien d'un contrôle efficace de l'immigration conformément au paragraphe 4, point 1, de l'annexe 2 de la loi britannique de 2018 sur la protection des données.
([4]) JO C 384 I du 12.11.2019, p. 1.
([5]) JO L 149 du 30.4.2021, p. 10, ELI: http://data.europa.eu/eli/agree_internation/2021/689(1)/oj.

(4) Pour se prononcer sur une éventuelle prorogation de la décision d'exécution (UE) 2021/1772, la Commission doit procéder à une évaluation afin de déterminer si la conclusion selon laquelle le Royaume-Uni assure un niveau de protection adéquat est toujours justifiée sur les plans factuel et juridique à la lumière de l'évolution de la situation depuis l'adoption de la décision d'exécution (UE) 2021/1772 en ce qui concerne les éléments énumérés à l'article 45, paragraphe 2, du règlement (UE) 2016/679.

(5) En particulier, le 23 octobre 2024, le gouvernement britannique a présenté au Parlement britannique le projet de loi sur les données (utilisation et accès) ([6]), qui contient des propositions de modifications du règlement général sur la protection des données du Royaume-Uni (RGPD britannique) et de la loi de 2018 sur la protection des données (DPA 2018) évalués dans la décision d'exécution (UE) 2021/1772. Le 24 juin 2025, la Commission a adopté la décision d'exécution (UE) 2025/1226 ([7]), qui a prolongé la validité de la décision d'exécution (UE) 2021/1772 pour une période de six mois, jusqu'au 27 décembre 2025. Cette prorogation technique limitée dans le temps a permis à la Commission de mener à bien son évaluation du caractère adéquat du niveau de protection des données à caractère personnel assuré par le Royaume-Uni en s'appuyant sur un cadre juridique stable, c'est-à-dire après l'achèvement du processus législatif concerné ([8]).

(6) Depuis l'adoption de la décision d'exécution (UE) 2021/1772, la Commission suit, de manière permanente, les évolutions pertinentes au Royaume-Uni ([9]). Conformément au considérant 281 de la décision d'exécution (UE) 2021/1772, une attention particulière a été accordée à l'application concrète des règles du Royaume-Uni concernant les transferts des données à caractère personnel aux pays tiers et à l'incidence qu'elle pourrait avoir sur le niveau de protection des données transférées en vertu de la décision d'exécution (UE) 2021/1772, à l'exercice effectif des droits individuels, y compris toute évolution pertinente de la législation et de la pratique concernant les exceptions ou restrictions à ces droits (notamment celle relative au maintien d'un contrôle efficace de l'immigration), ainsi qu'au respect des limitations et des garanties en ce qui concerne l'accès des pouvoirs publics. Entre autres éléments, l'évolution de la jurisprudence et le contrôle exercé par le Bureau du commissaire à l'information (ICO) et par d'autres organismes indépendants ont alimenté le suivi assuré par la Commission.

(7) Sur la base de l'évaluation de ces évolutions, y compris les modifications apportées au RGPD britannique et à la DPA 2018 par la loi sur les données (utilisation et accès), la Commission conclut que le Royaume-Uni continue d'assurer un niveau de protection adéquat des données à caractère personnel transférées dans le cadre du règlement (UE) 2016/679 de l'Union européenne vers le Royaume-Uni.

(8) La Commission conclut également que, à la lumière des modifications apportées aux dispositions pertinentes du droit britannique ([10]), il n'est plus justifié d'exclure du champ d'application de la décision d'exécution (UE) 2021/1772 les données à caractère personnel transférées à des fins de contrôle de l'immigration au Royaume-Uni ou qui relèvent par ailleurs du champ d'application de l'exemption de certains droits des personnes concernées aux fins du maintien d'un contrôle efficace de l'immigration (ci-après l'«exemption en matière d'immigration») conformément au paragraphe 4, point 1, de l'annexe 2 de la loi britannique sur la protection des données, comme expliqué au considérant 37 de la présente décision.

([6]) Disponible à l'adresse suivante: https://bills.parliament.uk/bills/3825/news.

([7]) Décision d'exécution (UE) 2025/1226 de la Commission du 24 juin 2025 modifiant la décision d'exécution (UE) 2021/1772 constatant, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par le Royaume-Uni (JO L, 2025/1226, 26.6.2025, ELI: http://data.europa.eu/eli/dec_impl/2025/1226/oj).

([8]) L'assentiment royal a été accordé à la loi sur les données (utilisation et accès) le 19 juin 2025.

([9]) Article 45, paragraphe 4, du règlement (UE) 2016/679.

([10]) En mai 2021, la Cour d'appel (Angleterre et pays de Galles) avait jugé l'exemption en matière d'immigration telle que formulée à l'époque au paragraphe 4, point 1, de l'annexe 2 de la loi britannique sur la protection des données incompatible avec le droit britannique, étant donné que cette mesure législative ne contenait pas de dispositions spécifiques établissant les garanties énumérées à l'article 23, paragraphe 2, du RGPD britannique. Afin de se conformer à cet arrêt, le gouvernement britannique a révisé l'exemption en matière d'immigration en adoptant la réglementation de 2022 relative à la loi de 2018 sur la protection des données (modification des exemptions prévues à l'annexe 2). Toutefois, l'exemption révisée a de nouveau été contestée au motif qu'elle ne satisfaisait pas à toutes les exigences de l'article 23, paragraphe 2, du RGPD britannique. Dans un arrêt du 11 décembre 2023, la Cour d'appel a déclaré une nouvelle fois incompatible avec l'article 23, paragraphe 2, du RGPD britannique l'exemption en matière d'immigration telle que révisée. Afin de se conformer à cet arrêt, le gouvernement britannique a ensuite adopté la réglementation de 2024 relative à la loi de 2018 sur la protection des données (modification des exemptions prévues à l'annexe 2), qui est entrée en vigueur le 8 mars 2024.

2. ÉVOLUTIONS PERTINENTES CONCERNANT LES RÈGLES APPLICABLES AU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

2.1. Le cadre de protection des données du Royaume-Uni

(9) Lorsque la décision d'exécution (UE) 2021/1772 a été adoptée, le cadre juridique en matière de protection des données à caractère personnel du Royaume-Uni se composait:

— du RGPD britannique ([11]), tel qu'il a été intégré dans le droit britannique en vertu de la loi de 2018 sur l'Union européenne (notification de retrait) ([12]) et modifié par la réglementation de 2019 sur la protection des données, la vie privée et les communications électroniques (modifications, etc.) (sortie de l'Union) (réglementation DPPEC) ([13]),

— et de la DPA 2018 ([14]), telle que modifiée par la réglementation DPPEC.

(10) Bien que ces deux lois, qui reflétaient étroitement les règles correspondantes applicables au sein de l'Union européenne, continuent de constituer la législation du Royaume-Uni en matière de protection des données, elles ont depuis lors fait l'objet de modifications limitées, traduisant le fait que le Royaume-Uni n'est plus soumis au droit de l'Union européenne.

(11) Premièrement, la loi de 2023 sur le droit de l'Union conservé (réforme et révocation) (REUL) ([15]) a précisé que les principes généraux du droit de l'Union ne feraient plus partie du droit national britannique après la fin de l'année 2023 ([16]). En outre, les juridictions du Royaume-Uni ne sont plus tenues d'interpréter le «droit assimilé» qui reste inchangé, qui était précédemment appelé «droit de l'Union conservé», conformément aux principes généraux du droit de l'Union; ledit droit doit plutôt être interprété de manière compatible avec le droit national britannique ([17]). Toutefois, le droit assimilé qui reste inchangé doit toujours être interprété par les juridictions compétentes du Royaume-Uni conformément à la jurisprudence pertinente de la Cour de justice de l'Union européenne rendue avant la fin de la période de transition ([18]), comme indiqué également au considérant 13 de la décision d'exécution (UE) 2021/1772. La DPA 2018 a été modifiée par la loi sur les données (utilisation et accès) afin de préciser les effets de la loi REUL sur la législation britannique en matière de protection des données. Par exemple, l'article 183A, paragraphe 1, de la DPA 2018 prévoit comme règle générale que toute nouvelle législation (adoptée le 20 août 2025 ou après cette date) qui introduit de nouvelles obligations ou de nouveaux pouvoirs en matière de traitement des données à caractère personnel est présumée être soumise à la législation britannique en matière de protection des données. Cela signifie que le cadre britannique de protection des données continue de prévaloir sur

([11]) General Data Protection Regulation, disponible à l'adresse suivante: https://www.legislation.gov.uk/eur/2016/679/contents.

([12]) European Union (Withdrawal) Act 2018, disponible à l'adresse suivante: https://www.legislation.gov.uk/ukpga/2018/16/contents, qui intégrait la législation de l'Union directement applicable au Royaume-Uni à la fin de la période de transition dans le droit britannique. Ce «droit de l'Union conservé» incluait l'intégralité du règlement (UE) 2016/679, y compris ses considérants [voir notes explicatives accompagnant la loi de 2018 sur l'Union européenne (notification de retrait), point 83, disponibles à l'adresse suivante: https://www.legislation.gov.uk/ukpga/2018/16/pdfs/ukpgaen_20180016_en.pdf]. Conformément à cette loi, le droit de l'Union conservé sans modifications devait être interprété par les juridictions du Royaume-Uni conformément à la jurisprudence pertinente de la Cour de justice de l'Union européenne et aux principes généraux du droit de l'Union étant donné qu'ils étaient d'effet immédiat avant la fin de la période de transition (respectivement appelés la «jurisprudence de l'Union conservée» et les «principes généraux du droit de l'Union conservés»).

([13]) Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, disponibles à l'adresse suivante: https://www.legislation.gov.uk/uksi/2019/419/contents/made, tels que modifiés par la réglementation DPPEC de 2020, disponible à l'adresse suivante: https://www.legislation.gov.uk/ukdsi/2020/9780348213522. La réglementation DPPEC modifie le règlement (UE) 2016/679, tel qu'il a été intégré dans le droit britannique par la loi de 2018 sur l'Union européenne (notification de retrait), la DPA 2018 et d'autres législations en matière de protection des données afin de les adapter au contexte national.

([14]) Data Protection Act 2018, disponible à l'adresse suivante: https://www.legislation.gov.uk/ukpga/2018/12/contents. Avant le retrait du Royaume-Uni de l'Union européenne et pendant la période de transition, la DPA 2018 établissait des règles nationales, lorsque le règlement (UE) 2016/679 le permettait, précisant et limitant l'application des règles du règlement (UE) 2016/679 et de la directive transposée (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, p. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj).

([15]) Disponible à l'adresse suivante: https://www.legislation.gov.uk/ukpga/2023/28.

([16]) Article 5 de la loi de 2018 sur l'Union européenne (notification de retrait), telle que modifiée par la loi REUL.

([17]) Article 5(A2) de la loi de 2018 sur l'Union européenne (notification de retrait), telle que modifiée par la loi REUL.

([18]) Article 6, paragraphes 3 et 7, de la loi de 2018 sur l'Union européenne (notification de retrait), telle que modifiée par la loi REUL.

d'autres législations. Conformément à l'article 183A, paragraphe 2, point b), de la DPA 2018, cette présomption peut être écartée si le Parlement britannique décide délibérément de le faire expressément dans la législation, en préservant la souveraineté parlementaire. Par ailleurs, l'article 186(2A) de la DPA 2018 précise que les limitations des droits des personnes concernées énumérées à l'article 186, paragraphe 3, de la DPA 2018 ne sont pas supplantées par l'article 186, paragraphe 1, de la DPA 2018, qui prévoit que les actes législatifs interdisant ou limitant la divulgation d'informations ne prévalent pas sur certains droits en matière de protection des données. Cela garantit, par exemple, que les limitations des droits des personnes concernées prévues par la DPA 2018 ne sont pas elles-mêmes visées par la «dérogation générale à la protection des données» prévue à l'article 186, paragraphe 1, de la DPA 2018.

(12) Deuxièmement, depuis l'adoption de la décision d'exécution (UE) 2021/1772, la législation du Royaume-Uni en matière de protection des données a été modifiée par la réglementation de 2023 relative à la protection des données (libertés et droits fondamentaux) (modification) ([19]). Cette réglementation définit les références aux droits fondamentaux ou aux libertés fondamentales contenues dans le RGPD britannique et la DPA 2018 [qui étaient précédemment définies comme des références aux droits fondamentaux et aux libertés fondamentales prévus par le droit de l'Union ([20])] comme des références aux droits consacrés par la convention européenne des droits de l'homme, qui ont été mis en œuvre dans le droit national britannique par la loi de 1998 sur les droits de l'homme ([21]). La loi de 1998 sur les droits de l'homme intègre dans le droit britannique les droits contenus dans la convention européenne des droits de l'homme. La loi sur les droits de l'homme confère à toute personne les libertés et droits fondamentaux prévus aux articles 2 à 12 et 14 de la convention européenne des droits de l'homme, aux articles 1er, 2 et 3 de son premier protocole et à l'article 1er de son treizième protocole, lus en combinaison avec les articles 16, 17 et 18 de ladite convention. Ces droits comprennent le droit au respect de la vie privée et familiale (et à la protection des données à caractère personnel, qui fait partie dudit droit) et le droit à un procès équitable ([22]).

(13) Enfin, le RGPD britannique et la DPA 2018 ont fait l'objet de réformes ciblées prévues par les parties 5 et 6 de la loi sur les données (utilisation et accès). Bien que le champ d'application de la loi sur les données (utilisation et accès) aille bien au-delà de la protection des données à caractère personnel, cette loi apporte des modifications limitées à plusieurs aspects du régime de protection des données, tels que, notamment, les règles relatives au traitement des données à des fins de recherche scientifique, les bases juridiques du traitement des données, les règles relatives au principe de limitation des finalités et les conditions régissant la prise de décision automatisée. En outre, la loi sur les données (utilisation et accès) apporte des modifications à la structure de gouvernance de l'ICO. Une fois mises en œuvre, ces mesures remplaceront l'ICO par une nouvelle entité, la commission de l'information. Le rôle et les fonctions de l'autorité de régulation en tant qu'autorité indépendante chargée de veiller à la protection des données au Royaume-Uni resteront inchangés. La loi investit également l'autorité de régulation de nouveaux pouvoirs d'exécution.

(14) La présente décision évalue les évolutions législatives, réglementaires et autres qui sont pertinentes pour la conclusion relative au niveau de protection assuré par le Royaume-Uni qui est formulée dans la décision d'exécution (UE) 2021/1772. L'évaluation effectuée dans la décision d'exécution (UE) 2021/1772 reste valable pour les aspects du cadre de protection des données du Royaume-Uni qui n'ont pas été modifiés ou concernés par d'autres évolutions depuis l'adoption de la décision d'exécution (UE) 2021/1772.

(15) Les évolutions législatives, réglementaires et autres qui sont pertinentes sont analysées en détail dans les sections suivantes sur la base du principe d'adéquation, selon lequel la Commission doit déterminer si le pays tiers en question assure un niveau de protection «essentiellement équivalent» à celui qui est garanti dans l'Union européenne ([23]). Comme l'a précisé la Cour de justice de l'Union européenne, il n'est pas nécessaire de constater un niveau de protection identique ([24]). En particulier, les moyens auxquels ce pays tiers a recours aux fins de la protection des données à caractère personnel peuvent être différents de ceux mis en œuvre au sein de l'Union, pour autant qu'ils s'avèrent, en pratique, effectifs afin d'assurer un niveau de protection adéquat ([25]). Le principe d'adéquation n'exige donc pas que l'on reproduise à l'identique les règles de l'Union. Il s'agit plutôt de déterminer si le système juridique étranger offre, dans son ensemble, par l'essence de ses droits en matière de protection des données et leur mise en œuvre effective, leur opposabilité et le contrôle de leur application, le niveau requis de protection ([26]).

([19]) Disponible à l'adresse suivante: https://www.gov.uk/government/publications/the-data-protection-fundamental-rights-and-freedoms-amendment-regulations-2023.

([20]) Les droits fondamentaux et les libertés fondamentales prévus par le droit de l'Union avaient été conservés dans le droit britannique en vertu de l'article 4 de la loi de 2018 sur l'Union européenne (notification de retrait), qui a été abrogé à la fin de 2023 par la loi REUL.

([21]) Article 2, paragraphe 3, de la réglementation de 2023 relative à la protection des données (libertés et droits fondamentaux) (modification).

([22]) Articles 6, 8, 10 et 13 de la CEDH (voir, également, annexe 1 de la loi de 1998 sur les droits de l'homme).

([23]) Considérant 104 du règlement (UE) 2016/679.

([24]) Arrêt de la Cour dans l'affaire C-362/14, Schrems (ci-après l'«arrêt Schrems I»), ECLI:EU:C:2015:650, point 73.

([25]) Arrêt Schrems I, point 74.

([26]) Voir communication de la Commission au Parlement européen et au Conseil intitulée «Échange et protection de données à caractère personnel à l'ère de la mondialisation» [COM(2017) 7 du 10.1.2017], section 3.1, p. 6 et 7, disponible à l'adresse suivante: https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52017DC0007&from=FR.

2.1.1. *Définitions*

(16) Les notions de base en matière de protection des données qui correspondent à la terminologie du règlement (UE) 2016/679 continuent de s'appliquer dans le régime de protection des données du Royaume-Uni. Ces notions ont été évaluées au considérant 23 de la décision d'exécution (UE) 2021/1772.

(17) Bien que la loi sur les données (utilisation et accès) laisse la grande majorité des définitions inchangée, elle a introduit des définitions spécifiques en ce qui concerne le traitement des données à caractère personnel à des fins scientifiques, historiques et statistiques à l'article 4, paragraphes 2, 3, 4 et 5, du RGPD britannique. Le paragraphe 2 définit le «traitement à des fins scientifiques» comme le traitement de données à caractère personnel effectué à des fins de recherches qui peuvent raisonnablement être qualifiées de scientifiques. Ces recherches peuvent être financées par des fonds publics ou privés et peuvent être menées en tant qu'activité commerciale ou non commerciale. Reflétant le contenu du considérant 159 du règlement (UE) 2016/679, le paragraphe 3 dresse une liste non exhaustive d'exemples d'activités de recherche considérées comme poursuivant des objectifs scientifiques, y compris le développement et la démonstration de technologies, la recherche fondamentale et la recherche appliquée. Le paragraphe 4 précise que la «recherche historique» inclut la recherche généalogique, qui est également reconnue comme une recherche à finalité historique au considérant 160 du règlement (UE) 2016/679. Enfin, le paragraphe 5 définit le traitement à des fins statistiques comme le traitement de données à des fins d'enquêtes statistiques ou de production de résultats statistiques, lorsque les données sont agrégées à un point tel qu'elles ne constituent plus des données à caractère personnel. En outre, les données traitées ou les informations qui en résultent ne doivent pas être utilisées pour prendre des décisions ou des mesures concernant une personne en particulier. Cette définition est conforme à la définition des fins statistiques énoncée au considérant 162 du règlement (UE) 2016/679.

(18) En conclusion, si les modifications apportées à l'article 4 du RGPD britannique ajoutent des définitions spécifiques en ce qui concerne le traitement des données à des fins scientifiques, historiques et statistiques, ces définitions sont conformes à la lettre et à l'esprit du règlement (UE) 2016/679 tels qu'ils ressortent des considérants 159, 160 et 162 susmentionnés.

(19) En ajoutant un paragraphe 6 à l'article 4 du RGPD britannique, la loi sur les données (utilisation et accès) a également établi un cadre spécifique pour l'obtention du consentement de la personne concernée pour le traitement de données à caractère personnel à des fins scientifiques. Dans des termes très semblables à ceux du considérant 33 du règlement (UE) 2016/679, où il est reconnu que, dans le domaine de la recherche scientifique, le consentement ne peut pas toujours être obtenu pour une finalité de traitement bien précise, la nouvelle disposition autorise des formes de consentement plus larges en permettant aux personnes concernées de donner un consentement valable même lorsqu'il n'est pas possible de pleinement cerner avec précision les finalités de la recherche au moment de la collecte des données, à condition que la demande de consentement soit conforme aux normes éthiques généralement reconnues applicables au domaine de recherche concerné. En tout état de cause, les personnes concernées doivent avoir la possibilité de donner leur consentement au traitement de données à caractère personnel uniquement pour des parties spécifiques de la recherche, dans la mesure du possible.

(20) Enfin, la loi sur les données (utilisation et accès) a précisé davantage les garanties précédemment énoncées à l'article 89 du RGPD britannique et à l'article 19 de la DPA 2018 pour le traitement des données à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, et ce dans un nouveau chapitre (le chapitre 8A) du RGPD britannique ([27]). Ces garanties sont semblables à celles qu'impose l'article 89 du règlement (UE) 2016/679 et comprennent l'obligation de prévoir des mesures techniques et organisationnelles afin de garantir le respect du principe de minimisation des données.

2.2. **Garanties, droits et obligations**

2.2.1. *Licéité et loyauté du traitement*

(21) Le cadre de protection des données du Royaume-Uni continue d'exiger que les données soient traitées de manière licite, loyale et légitime, comme indiqué aux considérants 24 à 26 de la décision d'exécution (UE) 2021/1772.

([27]) Articles 84A à 84D du RGPD britannique, tels qu'insérés par l'article 86 de la loi sur les données (utilisation et accès).

(22) Les principes de licéité et de loyauté, ainsi que les fondements du traitement licite, sont toujours garantis dans le droit du Royaume-Uni par l'article 5, paragraphe 1, point a), et l'article 6, paragraphe 1, du RGPD britannique, comme indiqué dans la décision d'exécution (UE) 2021/1772. Bien que ces dispositions restent largement identiques ([28]) aux dispositions correspondantes du règlement (UE) 2016/679, la loi sur les données (utilisation et accès) modifie d'abord l'article 6, paragraphe 1, du RGPD britannique en introduisant un motif licite supplémentaire pour le traitement des données à caractère personnel au titre de l'article 6, paragraphe 1, point ea) ([29]). En vertu de cette disposition, le traitement est licite si et dans la mesure où il «est nécessaire aux fins d'un intérêt légitime reconnu». Contrairement au fondement juridique de l'intérêt légitime prévu à l'article 6, paragraphe 1, point f), du RGPD britannique, le nouveau fondement juridique de l'intérêt légitime reconnu n'exige pas une mise en balance au cas par cas des intérêts légitimes du responsable du traitement et des intérêts ou libertés et droits fondamentaux de la personne concernée, l'objectif étant de conférer une plus grande sécurité juridique aux organismes de contrôle non publics. Le nouveau paragraphe 5 de l'article 6 du RGPD britannique précise que le traitement n'est nécessaire aux fins d'un intérêt légitime reconnu que s'il remplit une condition énoncée à l'annexe 1 ([30]), laquelle énumère ensuite les situations dans lesquelles le traitement est considéré comme nécessaire aux fins d'un intérêt légitime reconnu, par exemple lorsqu'il a lieu en réponse à une demande d'une autorité publique qui a besoin des données pour exécuter une mission d'intérêt public fondée sur une base juridique conforme à l'article 6, paragraphe 3, du RGPD britannique, lorsque le traitement est nécessaire pour garantir la sécurité nationale, protéger la sécurité publique ou à des fins de défense, pour répondre à une urgence, pour détecter ou prévenir des infractions pénales ou pour protéger des personnes vulnérables ([31]).

(23) Bien que la loi sur les données (utilisation et accès) élargisse donc la liste des fondements juridiques du traitement des données à caractère personnel dont le responsable du traitement peut se prévaloir, le nouveau fondement juridique de l'intérêt légitime reconnu est soumis à plusieurs limitations importantes. Premièrement, les intérêts légitimes reconnus se limitent à des situations spécifiques qui sont énumérées de manière exhaustive dans la loi. Deuxièmement, ce fondement juridique ne peut être invoqué par les autorités publiques dans l'exercice de leurs missions ([32]). Troisièmement, il ne concerne que des domaines dans lesquels il existe un intérêt public manifeste pour l'activité de traitement (conformément aux conditions énoncées à l'annexe 1), c'est-à-dire lorsque le traitement sert les objectifs énumérés à l'article 23 du RGPD britannique [qui correspond à l'article 23 du règlement (UE) 2016/679] et ne peut donc être invoqué à des fins commerciales. Quatrièmement, bien que la loi sur les données (utilisation et accès) investisse le secrétaire d'État du pouvoir de modifier la liste figurant à l'annexe 1 au

([28]) À des fins de clarification, la loi sur les données (utilisation et accès) insère également à l'article 6 du RGPD britannique un nouveau paragraphe, qui donne des exemples de types de traitement qui peuvent être considérés comme nécessaires aux fins d'un intérêt légitime au sens de l'article 6, paragraphe 1, point f), du RGPD britannique. Ces exemples (prospection, transmission de données au sein d'un groupe d'entreprises à des fins administratives et sécurité des réseaux et des systèmes d'information) sont également mentionnés aux considérants 47 et 48 du règlement (UE) 2016/679 comme des situations dans lesquelles le traitement serait considéré comme constituant un intérêt légitime du responsable du traitement.

([29]) Article 70, paragraphe 2, point b), de la loi sur les données (utilisation et accès). L'article 70, paragraphe 5, de la loi sur les données (utilisation et accès) a étendu au nouveau point ea) de l'article 6, paragraphe 1, du RGPD britannique le droit de s'opposer au traitement prévu à l'article 21 du RGPD britannique.

([30]) Article 70, paragraphe 4, de la loi sur les données (utilisation et accès).

([31]) Voir annexe 4 de la loi sur les données (utilisation et accès). Selon les autorités britanniques, les situations dans lesquelles des organismes non publics peuvent avoir besoin de traiter des données à caractère personnel pour prévenir ou détecter des infractions peuvent, par exemple, être celle d'une entreprise qui a connaissance de tentatives de piratage de ses systèmes informatiques, ou d'une banque ou d'un établissement financier qui a connaissance de tentatives frauduleuses d'ouverture d'un compte. Le traitement de données à caractère personnel par un organisme non public peut, par exemple, être nécessaire pour garantir la sécurité nationale ou la défense lorsqu'une organisation commerciale soupçonne que l'activité en ligne d'un client indique une implication dans des activités terroristes. L'ICO travaille actuellement à l'élaboration d'orientations spécifiques sur cette question, comprenant une définition des concepts pertinents. Par exemple, la «sécurité nationale» devrait couvrir la sécurité et le bien-être du Royaume-Uni dans son ensemble (population, institutions et système de gouvernement). Voir le projet d'orientations de l'ICO sur l'intérêt légitime reconnu, tel qu'il a été publié pour consultation publique, disponible à l'adresse suivante: https://ico.org.uk/for-organisations/recognised-legitimate-interest-guidance/.

([32]) Dernier alinéa de l'article 6, paragraphe 1, tel que modifié par l'article 70, paragraphe 2, point c), de la loi sur les données (utilisation et accès).

moyen d'un règlement ([33]), le secrétaire d'État ne peut établir un tel règlement qu'après avoir consulté l'ICO ([34]) et y ajouter un intérêt légitime reconnu que si le traitement est là encore nécessaire pour garantir un objectif d'intérêt public énuméré à l'article 23, paragraphe 1, points c) à j), du RGPD britannique ([35]). Enfin, comme le confirment également les orientations de l'ICO ([36]), les responsables du traitement qui s'appuient sur un intérêt légitime reconnu comme base juridique sont 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 réaliser l'intérêt légitime poursuivi.

(24) Deuxièmement, la loi sur les données (utilisation et accès) précise à l'article 6, paragraphe 3, à l'article 9, paragraphe 2, point g), et à l'article 10, paragraphe 1, du RGPD britannique, qui reflètent les dispositions correspondantes du règlement (UE) 2016/679, que le fondement du traitement des données à caractère personnel, du traitement portant sur des catégories particulières de données à caractère personnel et du traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions pour respecter une obligation légale ou pour exécuter une mission d'intérêt public peut être défini non seulement par le droit national, mais également par le droit international pertinent ([37]). Le droit international pertinent est ensuite limité par le nouvel article 9A du RGPD britannique, lu en combinaison avec l'annexe A1, à un seul accord, à savoir 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, qui a été signé le 3 octobre 2019 (ci-après l'«accord Royaume-Uni/États-Unis») ([38]). Les garanties prévues par cet accord ont été évaluées aux considérants 153 à 155 de la décision d'exécution (UE) 2021/1772 et leur mise en œuvre est analysée aux considérants 87 à 93 de la présente décision.

2.2.2. *Traitement portant sur des catégories particulières de données à caractère personnel*

(25) Le cadre de protection des données du Royaume-Uni continue de prévoir des garanties spécifiques pour le traitement portant sur des catégories particulières de données, lesquelles ont été évaluées aux considérants 27 à 42 de la décision d'exécution (UE) 2021/1772.

(26) Tant la définition des catégories particulières de données à caractère personnel que les règles spécifiques applicables au traitement de ces catégories de données qui sont incluses dans le RGPD britannique et dans la DPA 2018 restent en place. Dans le même temps, la loi sur les données (utilisation et accès) investit le secrétaire d'État de nouveaux pouvoirs l'habilitant à adopter des règlements pour ajouter des catégories particulières de données, adapter les conditions applicables à leur utilisation et ajouter de nouvelles définitions, si nécessaire ([39]). Il est important de noter qu'il n'est pas permis au secrétaire d'État de supprimer ou de modifier des catégories particulières de données existantes, ni de modifier les conditions régissant le traitement de ces catégories de données ([40]). Les nouveaux pouvoirs de réglementation permettent donc uniquement au gouvernement d'ajouter de nouvelles catégories de données sensibles et de déterminer les conditions applicables à leur traitement, l'objectif étant de faire en sorte que le gouvernement puisse réagir en tant que de besoin aux évolutions technologiques et sociétales futures.

(27) Par conséquent, ces modifications n'ont pas d'incidence sur le niveau de protection garanti pour les catégories particulières de données à caractère personnel, qui avait été jugé essentiellement équivalent à la protection assurée au sein de l'Union dans la décision d'exécution (UE) 2021/1772.

([33]) Avant d'arrêter des règlements, le secrétaire d'État doit tenir compte des effets de toute modification sur les intérêts et les libertés et droits fondamentaux des personnes concernées, ainsi que du fait que les enfants (le cas échéant) méritent une protection spécifique pour les données à caractère personnel les concernant. Les règlements doivent être établis par voie d'actes réglementaires et sont soumis à une procédure de ratification, ce qui signifie qu'ils nécessitent l'approbation expresse du Parlement britannique. Article 70, paragraphe 4, point 8), de la loi sur les données (utilisation et accès).

([34]) Article 182, paragraphe 2, de la DPA 2018.

([35]) Article 70, paragraphe 4, point 9), de la loi sur les données (utilisation et accès).

([36]) 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/?q=appropriate+policy.

([37]) Article 72 de la loi sur les données (utilisation et accès).

([38]) 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, disponible à l'adresse suivante: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf.

([39]) Article 74 de la loi sur les données (utilisation et accès). Ces règlements sont soumis à une procédure de ratification, ce qui signifie qu'ils nécessitent l'approbation expresse du Parlement britannique.

([40]) Voir nouvel article 11A, paragraphe 1, point b), et paragraphe 2, du RGPD britannique, ainsi que notes explicatives accompagnant le projet de loi sur les données (utilisation et accès), point 571, disponibles à l'adresse suivante: https://publications.parliament.uk/pa/bills/cbill/59-01/0179/en/240179en.pdf.

2.2.3. *Limitation des finalités*

(28) Le régime de protection des données à caractère personnel du Royaume-Uni continue d'exiger que les données soient traitées dans un but précis et ne soient utilisées ultérieurement que dans la mesure où cela n'est pas incompatible avec la finalité initiale du traitement, comme indiqué aux considérants 43 à 48 de la décision d'exécution (UE) 2021/1772.

(29) Premièrement, la loi sur les données (utilisation et accès) apporte quelques modifications ciblées au principe de limitation des finalités énoncé à l'article 5, paragraphe 1, point b), du RGPD britannique. Ces modifications clarifient l'application de ce principe sans en modifier la substance. L'article 71, points 1, 2 et 3, de la loi sur les données (utilisation et accès) précise que le principe de limitation des finalités s'applique lorsque les données sont collectées auprès de la personne concernée ou d'une autre manière, qu'il ne s'applique que lorsque les données à caractère personnel sont traitées ultérieurement par le même responsable du traitement ou pour son compte (c'est-à-dire qu'il ne s'applique pas en cas de changement de responsable du traitement) et que le traitement n'est pas licite au seul motif qu'il est compatible avec les finalités pour lesquelles les données à caractère personnel ont été collectées.

(30) Deuxièmement, la loi sur les données (utilisation et accès) clarifie les règles relatives au traitement ultérieur des données à caractère personnel en les regroupant dans le nouvel article 8A du RGPD britannique, lequel contient l'intégralité du régime applicable au traitement ultérieur des données à caractère personnel. L'article 8A, paragraphe 2, du RGPD britannique énumère les éléments à prendre en considération pour déterminer si une nouvelle finalité de traitement est compatible avec la finalité initiale. Ces éléments étaient précédemment énumérés à l'article 6, paragraphe 4, du RGPD britannique, qui correspond à l'article 6, paragraphe 4, du règlement (UE) 2016/679 ([41]). L'article 8A, paragraphe 3, du RGPD britannique regroupe en une seule disposition les situations dans lesquelles le traitement des données à caractère personnel pour une nouvelle finalité doit être considéré comme compatible avec la finalité initiale. Cette disposition couvre les situations dans lesquelles la personne concernée consent au traitement des données à caractère personnel pour la nouvelle finalité ou dans lesquelles le traitement est nécessaire pour garantir un objectif énuméré à l'article 23, paragraphe 1 ([42]), ou encore dans lesquelles le traitement est effectué à des fins de recherche scientifique ou historique, à des fins archivistiques dans l'intérêt public ou à des fins statistiques ([43]). Enfin, la loi sur les données (utilisation et accès) précise que tout traitement effectué pour garantir ou démontrer que le traitement est conforme aux principes de protection des données énoncés à l'article 5, paragraphe 1, du RGPD britannique est considéré comme compatible avec la finalité initiale. Les situations susmentionnées continuent de correspondre à ce qui est considéré comme un traitement ultérieur compatible dans le règlement (UE) 2016/679.

(31) Troisièmement, la loi sur les données (utilisation et accès) intègre également à l'article 8A, paragraphe 3, point d), du RGPD britannique de nouvelles situations dans lesquelles le traitement ultérieur des données à caractère personnel pour une nouvelle finalité est considéré comme compatible avec la finalité initiale. Ces situations sont énumérées à l'annexe 2 du RGPD britannique ([44]) et il s'agit, par exemple, des situations dans lesquelles le traitement a lieu en réponse à une demande d'une autorité publique qui a besoin des données pour exécuter une mission d'intérêt public fondée sur une base juridique conforme à l'article 6, paragraphe 3, du RGPD britannique, ou dans lesquelles le traitement est nécessaire pour protéger la sécurité publique ou répondre à une urgence, pour la détection et la prévention des infractions pénales ainsi que les enquêtes en la matière, pour la sauvegarde des intérêts vitaux de la personne concernée et d'autres personnes, pour la protection des personnes vulnérables, à des fins fiscales ou pour le respect d'une obligation légale ([45]).

(32) Bien que la loi sur les données (utilisation et accès) étende donc la liste des situations dans lesquelles le traitement ultérieur pour une finalité différente est considéré comme compatible avec la finalité initiale du traitement, cette extension est soumise à d'importantes limitations. Premièrement, elle est limitée à des situations spécifiques qui sont énumérées de manière exhaustive dans la loi. Deuxièmement, elle ne concerne que des domaines dans lesquels il existe un intérêt public manifeste pour l'activité de traitement, c'est-à-dire lorsque le traitement ultérieur sert les

([41]) Comme dans le règlement (UE) 2016/679, ces éléments comprennent l'existence éventuelle d'un lien entre la finalité initiale et la nouvelle finalité, le contexte dans lequel les données à caractère personnel ont été collectées, y compris la relation entre la personne concernée et le responsable du traitement, la nature du traitement et la question de savoir s'il porte sur des catégories particulières de données, les conséquences possibles du traitement envisagé pour la personne concernée et l'existence de garanties appropriées.

([42]) Voir, également, article 6, paragraphe 4, du règlement (UE) 2016/679.

([43]) Considérant 50 du règlement (UE) 2016/679.

([44]) L'annexe 2 est insérée dans le RGPD britannique par l'annexe 5 de la loi sur les données (utilisation et accès); voir article 71, paragraphe 6, de cette loi.

([45]) Voir annexe 5 de la loi sur les données (utilisation et accès).

objectifs énumérés à l'article 23 du RGPD britannique [qui correspond à l'article 23 du règlement (UE) 2016/679]. L'invocation à des fins commerciales n'est donc pas autorisée. Troisièmement, bien que la loi sur les données (utilisation et accès) investisse le secrétaire d'État du pouvoir de modifier la liste figurant à l'annexe 2 au moyen d'un règlement ([46]), le secrétaire d'État ne peut y ajouter des types de traitement que si le traitement est là encore nécessaire pour garantir un objectif d'intérêt public énuméré à l'article 23, paragraphe 1, points c) à j), du RGPD britannique ([47]). Quatrièmement, lorsque la collecte de données à caractère personnel par le responsable du traitement est fondée sur le consentement de la personne concernée, le traitement pour une nouvelle finalité dans les situations énumérées à l'annexe 2 n'est considéré comme compatible avec la finalité initiale que si l'on ne peut raisonnablement s'attendre à ce que le responsable du traitement obtienne un nouveau consentement de la personne concernée ([48]).

2.2.4. *Droits individuels*

(33) En vertu du cadre de protection des données à caractère personnel applicable au Royaume-Uni, les personnes concernées continuent de bénéficier des mêmes droits individuels que ceux que prévoit le règlement (UE) 2016/679, sans modifications substantielles ([49]), et elles peuvent opposer ces droits au responsable du traitement ou au sous-traitant. Il s'agit en particulier du droit d'accès aux données, du droit de s'opposer au traitement et du droit à la rectification et à l'effacement des données, comme indiqué aux considérants 51 à 54 de la décision d'exécution (UE) 2021/1772.

(34) Premièrement, la loi sur les données (utilisation et accès) clarifie certaines modalités d'exercice de ces droits. D'une part, elle précise, par une modification apportée à l'article 12 et l'ajout d'un nouvel article (l'article 12A) dans le RGPD britannique ([50]), les délais dans lesquels les responsables du traitement doivent répondre aux demandes de la personne concernée. Plus précisément, l'article 12 du RGPD britannique est modifié de manière que le responsable du traitement ne soit plus tenu de fournir des informations sur les mesures prises (ou sur les raisons pour lesquelles aucune mesure n'a été prise) en réponse à une demande d'une personne concernée conformément aux articles 15 à 22 du RGPD britannique «dans un délai d'un mois à compter de la réception de la demande», mais «avant la fin du délai applicable». Le délai applicable est défini plus en détail dans le nouvel article 12A du RGPD britannique comme étant un délai d'un mois à compter du moment pertinent, à savoir le moment auquel le responsable du traitement reçoit la demande, le moment auquel le responsable du traitement reçoit toute information demandée dans le cadre d'une demande au titre de l'article 12, paragraphe 6, du RGPD britannique ou le moment auquel des frais appliqués en rapport avec la demande au titre de l'article 12, paragraphe 5, du RGPD britannique ont été payés, la date la plus tardive étant retenue ([51]). L'article 12A, paragraphe 3, autorise en outre le responsable du traitement à prolonger le délai applicable de deux mois lorsque cela est nécessaire eu égard à la complexité des demandes de la personne concernée ou au nombre de demandes. D'autre part, en ce qui concerne uniquement le droit d'accès aux informations et aux données à caractère personnel, la loi sur les données (utilisation et accès) modifie l'article 15 du RGPD britannique pour intégrer la clarification apportée par la jurisprudence nationale — en s'appuyant sur le principe de proportionnalité du droit de l'Union — qui précise que les responsables du traitement ne doivent effectuer que des recherches raisonnables et proportionnées pour obtenir les informations et les données à caractère personnel demandées ([52]). La nouvelle disposition devrait être interprétée conformément à la jurisprudence existante, qui prévoit que «[…] ce qui est mis en balance dans l'examen de proportionnalité est l'objet final de la recherche, à savoir l'avantage potentiel que la fourniture d'informations pourrait apporter à la personne concernée, par rapport aux moyens par lesquels ces informations sont obtenues. Il s'agira d'évaluer dans chaque cas particulier si des efforts disproportionnés seront nécessaires pour trouver et fournir les informations par rapport aux avantages que cela pourrait apporter à la personne concernée» ([53]).

([46]) Paragraphe 5 de l'article 8A du RGPD britannique, tel qu'inséré par l'article 71, paragraphe 1, de la loi sur les données (utilisation et accès).

([47]) Paragraphe 6 de l'article 8A du RGPD britannique, tel qu'inséré par l'article 71, paragraphe 1, de la loi sur les données (utilisation et accès).

([48]) Paragraphe 4, point b), de l'article 8A du RGPD britannique, tel qu'inséré par l'article 71, paragraphe 1, de la loi sur les données (utilisation et accès).

([49]) L'article 31 de la loi de 2024 sur les victimes et les détenus (VAP) a inséré dans le droit à l'effacement prévu à l'article 17 du RGPD britannique un motif supplémentaire, en vertu duquel les personnes concernées peuvent demander aux responsables du traitement l'effacement des données à caractère personnel les concernant lorsqu'elles ont été traitées à la suite d'une allégation infondée formulée à leur encontre par une personne malveillante. Une personne est considérée comme «malveillante» si elle a été condamnée pour une infraction visée à l'article 31, paragraphe 3, de la VAP (harcèlement, par exemple) ou fait l'objet d'une ordonnance de protection. La VAP est disponible à l'adresse suivante: https://www.legislation.gov.uk/ukpga/2024/21/contents. En outre, l'article 77 de la loi sur les données (utilisation et accès) modifie le droit à l'information prévu à l'article 13 du RGPD britannique de telle sorte que le responsable du traitement n'est plus tenu d'informer la personne concernée du traitement ultérieur des données à caractère personnel la concernant pour une nouvelle finalité lorsque ce traitement est effectué à des fins de recherche scientifique ou historique, à des fins archivistiques dans l'intérêt public ou à des fins statistiques, lorsque ce traitement est effectué conformément aux garanties spécifiques énoncées au nouvel article 84B du RGPD britannique, et lorsque la fourniture d'informations serait impossible ou disproportionnée.

([50]) Article 76 de la loi sur les données (utilisation et accès).

([51]) Paragraphes 1 et 2 de l'article 12A du RGPD britannique, tels qu'insérés par l'article 76 de la loi sur les données (utilisation et accès).

([52]) Paragraphe 1A de l'article 15 du RGPD britannique, tel qu'inséré par l'article 78 de la loi sur les données (utilisation et accès).

([53]) Dawson-Dammer contre Taylor Wessing LLP [2017] EWCA Civ 74.

(35) Par conséquent, si les délais de réponse aux demandes des personnes concernées et les obligations spécifiques des responsables du traitement en ce qui concerne le droit d'accès sont soumis à des règles plus détaillées, le système en place au Royaume-Uni continue de garantir que les demandes des personnes concernées doivent être traitées dans des délais raisonnables, définis sur la base de facteurs objectifs. En outre, les obligations matérielles qui incombent aux responsables du traitement lorsqu'ils répondent à une demande d'accès sont encadrées par des normes juridiques établies qui tiennent également compte des intérêts de la personne concernée. Enfin, les orientations actuelles de l'ICO précisent déjà qu'un responsable du traitement n'est pas tenu d'effectuer des recherches qui seraient déraisonnables ou disproportionnées par rapport à l'importance de donner accès aux informations ([54]).

(36) Les restrictions à ces droits individuels énoncées dans la DPA 2018, qui s'inscrivent dans le cadre de l'article 23 du RGPD britannique, ainsi que les limitations et garanties qui encadrent l'application de ces restrictions, décrites en détail aux considérants 55 à 67 de la décision d'exécution (UE) 2021/1772, sont toujours en place dans le cadre du Royaume-Uni ([55]).

(37) Pour ce qui est plus précisément de la limitation concernant les données à caractère personnel traitées aux fins du maintien d'un contrôle efficace de l'immigration, ou de la détection des activités qui compromettraient le maintien d'un contrôle efficace de l'immigration et des enquêtes en la matière, dans la mesure où l'application de ces dispositions est susceptible de porter préjudice à l'une de ces finalités (l'exemption en matière d'immigration) ([56]), le gouvernement britannique a modifié le point 4 de l'annexe 2 de la DPA 2018 en adoptant la réglementation de 2022 relative à la loi de 2018 sur la protection des données (modification des exemptions prévues à l'annexe 2) ([57]) et la réglementation de 2024 relative à la loi de 2018 sur la protection des données (modification des exemptions prévues à l'annexe 2) ([58]), qui vient compléter la réglementation de 2022 ([59]). Les modifications intègrent dans les points 4A et 4B de l'annexe 2 de la DPA 2018 les garanties pour l'exercice de l'exemption en matière d'immigration requises par l'article 23, paragraphe 2, du RGPD britannique. En particulier, il est exigé i) que l'exemption en matière d'immigration soit uniquement invoquée au cas par cas et séparément pour chacune des dispositions pertinentes du RGPD britannique et à nouveau à chaque fois que le secrétaire d'État envisage de ne pas appliquer ou d'appliquer de manière limitée l'une des dispositions pertinentes du RGPD britannique ([60]), ii) qu'il soit tenu compte des droits et libertés de la personne concernée ainsi que de ses vulnérabilités potentielles lors de l'application de l'exemption en matière d'immigration ([61]), iii) que le secrétaire d'État consigne dans un registre les cas d'application de l'exemption en matière d'immigration et qu'il informe la personne concernée de son application (sauf dans des circonstances spécifiques si l'information risque de compromettre l'objectif de l'exemption) ([62]), et iv) qu'il soit précisé que l'application de l'exemption en matière d'immigration est limitée au traitement des données à caractère personnel par le secrétaire d'État ([63]), à savoir, dans la pratique, par le ministère de l'intérieur pour les fonctions visées au point 4.1 de l'annexe 2 de la DPA 2018. En outre, les modifications expliquent comment procéder à l'exercice de mise en balance pour déterminer si l'exercice des droits des personnes concernées est susceptible de porter préjudice à un contrôle effectif de l'immigration et s'il est nécessaire et proportionné de limiter ces droits en conséquence.

([54]) Disponibles à l'adresse suivante: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/how-do-we-find-and-retrieve-the-relevant-information/.

([55]) L'article 88, paragraphe 2, de la loi sur les données (utilisation et accès) apporte une légère modification à l'article 26, paragraphe 2, point f), de la DPA 2018 (exemption en matière de sécurité et de défense nationales), afin de préciser que le droit d'introduire une réclamation auprès du commissaire en vertu de l'article 77 du RGPD britannique ne fait pas partie des dispositions dont l'application peut être limitée à des fins de sécurité ou de défense nationales.

([56]) Lors de l'adoption de la décision d'exécution (UE) 2021/1772, la question de la validité et de l'interprétation de l'exemption en matière d'immigration en droit britannique n'était pas encore réglée, car, dans une décision du 26 mai 2021, la Cour d'appel (Angleterre et pays de Galles) avait conclu que cette exemption, telle qu'elle figurait à l'époque dans la DPA 2018, était incompatible avec le droit britannique, en ce qu'elle ne contenait pas de dispositions spécifiques énonçant les garanties énumérées à l'article 23, paragraphe 2, du RGPD britannique, qui correspond à l'article 23, paragraphe 2, du règlement (UE) 2016/679. Pour cette raison, les données à caractère personnel transférées à des fins de contrôle de l'immigration au Royaume-Uni ou qui relèvent par ailleurs du champ d'application de l'exemption en matière d'immigration avaient été exclues du champ d'application de la décision d'exécution (UE) 2021/1772.

([57]) Cette réglementation est entrée en vigueur le 31 janvier 2022 et est disponible à l'adresse suivante: https://www.legislation.gov.uk/uksi/2022/76/contents/made.

([58]) Cette réglementation est entrée en vigueur le 8 mars 2024 et est disponible à l'adresse suivante: https://www.legislation.gov.uk/uksi/2024/342/contents/made.

([59]) L'exemption en matière d'immigration telle que révisée par la réglementation de 2022 a de nouveau été contestée dans le cadre d'un contrôle juridictionnel, au motif qu'elle ne satisfaisait toujours pas à toutes les exigences de l'article 23, paragraphe 2, du RGPD britannique. En décembre 2023, la Cour d'appel a jugé qu'elle était incompatible avec les exigences de l'article 23, paragraphe 2, du RGPD britannique. À la suite de cet arrêt, la réglementation de 2024 est venue compléter la réglementation de 2022 et apporter de nouvelles modifications à l'exemption en matière d'immigration.

([60]) Annexe 2, point 4A, 2), de la DPA 2018.

([61]) Annexe 2, points 4AB, 3) et 4AB,4), de la DPA 2018. Le Bureau du commissaire à l'information a été consulté sur le projet de réglementation de 2024 et a publiquement déclaré qu'il en était satisfait. La lettre publiée en réponse à la consultation et confirmant cet avis est disponible à l'adresse suivante: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/02/ico-responds-to-home-office-s-draft-regulations-to-the-immigration-exemption/.

([62]) Annexe 2, points 4B, 1), et 4B, 2), de la DPA 2018.

([63]) Annexe 2, point 4, 1), de la DPA 2018.

(38) Par ailleurs, l'ICO a publié des orientations détaillées concernant l'utilisation de cette limitation spécifique ([64]). Ces orientations mentionnent notamment ce qui suit: «Il n'y a pas lieu d'appliquer l'exemption en matière d'immigration de manière généralisée pour limiter […] des droits relatifs à toutes les données que vous détenez. La portée de cette exemption se limite aux droits qui, s'ils étaient exercés pour les données détenues, porteraient préjudice aux finalités définies en matière d'immigration. […]. Par conséquent, en principe, il convient que le responsable du traitement satisfasse, dans la mesure du possible, aux exigences du règlement (UE) 2016/679 et de la DPA. […] Le critère du préjudice est soumis à un seuil élevé et il n'y a pas lieu d'appliquer l'exemption de manière généralisée. […] Il convient de déterminer si l'application de l'exemption constitue une réponse proportionnée à la demande de protection des données de la personne concernée. Bien qu'il soit possible de considérer qu'il existe un besoin social impérieux d'appliquer l'exemption en matière d'immigration, il faut aussi examiner si ce besoin l'emporte sur l'obligation envers les personnes concernées qui vous incombe au titre du règlement (UE) 2016/679. Ces personnes disposent de droits sur les données à caractère personnel les concernant dont vous devez tenir compte en toutes circonstances, en particulier en ce qui concerne le droit d'accès. Il importe donc, dans chaque cas, de déterminer si les droits de la personne concernée à la protection des données la concernant l'emportent sur le risque de préjudice constaté. L'application de l'exemption doit être proportionnée aux circonstances et il est nécessaire de procéder à chaque fois à un examen rigoureux et de documenter chaque cas.»

(39) Dans l'ensemble, l'exemption en matière d'immigration prévue au paragraphe 4 de l'annexe 2 de la DPA 2018, telle que révisée par le gouvernement britannique en 2022 et 2024 et telle qu'interprétée par la jurisprudence ([65]) et les orientations de l'ICO, est soumise à un certain nombre de conditions strictes qui encadrent son application et sont très semblables aux conditions fixées par le droit de l'Union, notamment l'article 23 du règlement (UE) 2016/679, pour la limitation des droits et obligations en matière de protection des données pour des motifs importants d'intérêt public, tels que le contrôle de l'immigration.

2.2.5. *Limitations concernant les transferts ultérieurs*

(40) Le niveau de protection conféré aux données à caractère personnel qui sont transférées de l'Union européenne vers des responsables du traitement ou des sous-traitants au Royaume-Uni continue de ne pas être compromis par le transfert ultérieur de ces mêmes données vers des destinataires se trouvant dans un pays tiers. 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 du règlement (UE) 2016/679, comme indiqué aux considérants 74 à 82 de la décision d'exécution (UE) 2021/1772.

(41) Bien que la loi sur les données (utilisation et accès) ait modifié le chapitre 5 du RGPD britannique concernant les transferts de données à caractère personnel vers des pays tiers ou des organisations internationales, elle maintient les exigences essentielles selon lesquelles les données à caractère personnel ne peuvent être transférées vers un pays tiers ou une organisation internationale que si le transfert est fondé i) sur des règlements approuvant le transfert (nouvelle terminologie pour ce qui était auparavant les «règlements d'adéquation»), ii) sur des garanties appropriées ou iii) sur une dérogation pour cause de circonstances particulières. Ces principes généraux applicables aux transferts de données se reflètent dans le nouvel article 44A du RGPD britannique, qui remplace l'article 44 ([66]) et qui précise également que les transferts de données à caractère personnel vers un pays tiers ou une organisation internationale ne sont autorisés que si le transfert est effectué conformément aux autres dispositions du RGPD britannique.

(42) En ce qui concerne plus particulièrement les règlements approuvant un transfert, l'article 45A, paragraphe 2, du RGPD britannique précise que le secrétaire d'État ne peut établir de tels règlements que s'il considère que le critère de la protection des données est rempli. Cela signifie que la possibilité, introduite à l'article 45A, paragraphe 3, du RGPD britannique, pour le secrétaire d'État de tenir compte de l'opportunité de faciliter les flux de données lors de l'adoption de tels règlements est toujours subordonnée à la condition que le critère de la protection des données soit rempli. La norme juridique relative au critère de la protection des données à remplir est énoncée dans le nouvel article 45B, paragraphe 1, du RGPD britannique, qui exige que le niveau de protection des personnes concernées assuré dans les pays destinataires ou par les organisations internationales ne soit pas sensiblement inférieur à la norme prévue pour les personnes concernées par la législation britannique pertinente en matière de protection des données. L'article 45B, paragraphe 2, du RGPD britannique dresse une liste non exhaustive d'éléments à prendre en considération pour évaluer si ce critère est rempli, tels que le respect de l'état de droit et des droits de l'homme, l'existence d'une autorité chargée de la protection des données et ses pouvoirs, les modalités de recours juridictionnel ou extrajudiciaire, les règles relatives au transfert de données à caractère personnel du pays ou de

([64]) Disponibles à l'adresse suivante: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/immigration-exemption-a-guide/.

([65]) Arrêt Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin), points 40 et 41.

([66]) Article 85 et annexe 7 de la loi sur les données (utilisation et accès).

l'organisation vers d'autres pays ou organisations internationale, les obligations internationales pertinentes du pays ou de l'organisation, ainsi que la constitution, les traditions et la culture du pays ou de l'organisation. Bien qu'il reformule la liste des éléments pertinents prévue à l'ancien article 45 du RGPD britannique, le nouvel article 45B, paragraphe 2, conserve les éléments essentiels de cette liste et reste donc proche de ce qui est prévu au chapitre V du règlement (UE) 2016/679. En outre, les autorités britanniques ont confirmé que le secrétaire d'État tiendra compte d'éléments qui ne sont pas énumérés à l'article 45B, paragraphe 2, tels que les lois et pratiques d'un pays tiers concernant la manière dont les autorités publiques accèdent aux données à caractère personnel à des fins telles que la sécurité nationale ou l'application des lois, dans la mesure où ces éléments ont une incidence sur le niveau global de protection. Par ailleurs, les autorités britanniques considèrent que la jurisprudence pertinente du pays tiers sera un élément essentiel lors de l'examen des questions énumérées de manière non exhaustive à l'article 45B, paragraphe 2, du RGPD britannique.

(43) Les règlements approuvant un transfert continuent d'être soumis aux règles de procédure «générales» prévues à l'article 182 de la DPA 2018, comme indiqué au considérant 77 de la décision d'exécution (UE) 2021/1772. Dans le cadre de cette procédure, le secrétaire d'État doit consulter le commissaire à l'information lorsqu'il propose à l'adoption des règlements d'adéquation ([67]). Une fois adoptés par le secrétaire d'État, ces règlements sont présentés au Parlement et sont soumis à la procédure de «résolution négative» dans le cadre de laquelle les deux chambres du Parlement peuvent examiner les règlements et déposer une motion en vue de leur annulation dans un délai de 40 jours ([68]).

(44) En ce qui concerne les garanties appropriées, le nouveau paragraphe 1A de l'article 46 du RGPD britannique prévoit que ces transferts ne peuvent avoir lieu que si les instruments disponibles en vertu de l'article 46, paragraphes 2 et 3 ([69]), du RGPD britannique prévoient des garanties pertinentes et si le responsable du traitement, le sous-traitant ou les organismes publics applicables, agissant de manière raisonnable et proportionnée, considèrent que le critère de la protection des données est rempli. Les nouveaux paragraphes 6 et 7 précisent que le critère de la protection des données est rempli si, grâce aux garanties requises, le niveau de protection prévu pour les personnes concernées n'est pas sensiblement inférieur, après le transfert, à la norme prévue par la législation britannique pertinente en matière de protection des données. Autrement dit, comme c'est le cas en vertu du règlement (UE) 2016/679, les mêmes normes juridiques s'appliquent tant aux règlements approuvant un transfert qu'aux garanties appropriées. Selon ce même paragraphe, ce qui est raisonnable et proportionné doit être déterminé au regard de toutes les circonstances, ou circonstances probables, entourant le transfert ou le type de transfert, notamment la nature et le volume des données à caractère personnel transférées.

(45) En ce qui concerne les dérogations pour cause de circonstances particulières, s'agissant des conditions dans lesquelles ces dérogations peuvent être appliquées, plusieurs modifications techniques sont apportées à l'article 49 du RGPD britannique pour aligner cette disposition sur les modifications apportées à d'autres dispositions, mais sans avoir d'incidence sur le niveau de protection des données à caractère personnel assuré par le Royaume-Uni. En outre, un nouveau paragraphe (le paragraphe 4A) est inséré pour reproduire l'effet de l'article 18, paragraphe 1, de la DPA 2018 qui investit le secrétaire d'État du pouvoir de préciser, par des règlements, les circonstances dans lesquelles les transferts de données sont jugés nécessaires pour des motifs d'intérêt public. Enfin, un nouvel article (l'article 49A) reproduit l'effet de l'article 18, paragraphe 2, de la DPA 2018 qui habilite le secrétaire d'État à imposer par la voie de règlements des restrictions aux transferts de données lorsque ceux-ci ne sont pas approuvés en vertu de l'article 45A (transferts approuvés par des règlements) et lorsque cela est jugé nécessaire pour des motifs importants d'intérêt public.

(46) En ce qui concerne la mise en œuvre des règles britanniques applicables aux transferts internationaux, plusieurs évolutions ont eu lieu depuis l'adoption de la décision d'exécution (UE) 2021/1772.

([67]) Voir le protocole d'accord entre le secrétaire d'État au ministère du numérique, de la culture, des médias et du sport (Department for Digital, Culture, Media and Sport) et le bureau du commissaire à l'information sur le rôle de l'ICO dans le cadre de la nouvelle évaluation de l'adéquation au Royaume-Uni, disponible à l'adresse suivante: https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([68]) Si une telle motion est adoptée, les règlements cesseront à terme de produire tout autre effet juridique.

([69]) Les instruments de transfert disponibles en vertu de l'article 46, paragraphes 2 et 3, du RGPD britannique consistent en des instruments juridiquement contraignants et exécutoires entre les autorités ou organismes publics, des règles d'entreprise contraignantes conformément à l'article 47 du RGPD britannique, des clauses types de protection des données spécifiées dans des règlements adoptés par le secrétaire d'État ou dans un document émis par la commission de l'information, des codes de conduite approuvés et des mécanismes de certification approuvés.

(47) Pour ce qui est des règlements approuvant les transferts, deux nouveaux règlements ont été adoptés jusqu'à présent pour refléter des décisions d'adéquation qui sont en vigueur au sein de l'Union également. Ils concernent ainsi les transferts vers la République de Corée et les transferts vers des entités commerciales qui ont adhéré à l'extension au Royaume-Uni du cadre de protection des données UE - États-Unis. Les règlements d'adéquation concernant la République de Corée ([70]) sont entrés en vigueur le 19 décembre 2022 et autorisent le transfert de données à caractère personnel du Royaume-Uni vers la République de Corée. L'extension au Royaume-Uni du cadre de protection des données UE - États-Unis, pour laquelle les règlements pertinents ([71]) sont entrés en vigueur le 12 octobre 2023, permet la libre circulation des données à caractère personnel vers des organisations américaines certifiées.

(48) En ce qui concerne les garanties appropriées, le Royaume-Uni a publié ses propres clauses contractuelles types en matière de protection des données, l'accord international sur le transfert de données ([72]), et un addendum aux clauses contractuelles types de l'Union, qui sont entrés en vigueur en mars 2022. L'accord international sur le transfert de données prévoit un mécanisme spécifique pour le Royaume-Uni afin de veiller à ce que des garanties appropriées soient en place pour le transfert de données à caractère personnel et présente plusieurs similitudes avec les clauses contractuelles types de l'Union. L'addendum, publié par l'ICO, permet aux responsables du traitement et aux sous-traitants au Royaume-Uni de s'appuyer sur les clauses contractuelles types de l'Union dans le cadre du RGPD britannique pour les transferts internationaux. L'ICO a également publié un outil d'évaluation des risques de transfert afin d'aider les organisations britanniques à évaluer les risques associés aux transferts internationaux.

(49) Le Royaume-Uni a en outre rationalisé le processus d'approbation des règles d'entreprise contraignantes en adoptant de nouvelles orientations et de nouvelles possibilités pour l'approbation des règles d'entreprise contraignantes. En juillet 2022, l'ICO a publié des orientations et des tableaux de référence afin d'expliquer l'approche du Royaume-Uni pour les règles d'entreprise contraignantes après le Brexit et, en décembre 2023, un addendum aux règles d'entreprise contraignantes de l'Union a été publié afin de garantir que les règles d'entreprise contraignantes approuvées au titre du cadre de l'Union sont exécutoires au Royaume-Uni ([73]).

(50) Enfin, en juillet 2023, le Royaume-Uni est devenu un membre associé du Forum mondial sur les règles relatives aux transferts transfrontaliers de données (forum CBPR) ([74]). Il est important de noter que ce statut de membre associé n'entraîne aucune facilitation des transferts de données du Royaume-Uni vers d'autres membres du forum CBPR. Le Royaume-Uni a précisé que tout transfert de données à caractère personnel du Royaume-Uni vers des pays tiers ou des organisations internationales doit satisfaire aux conditions énoncées dans la législation britannique, telles que décrites ci-dessus, en particulier le critère de la protection des données, qui exige que les normes de protection accordées ne soient pas «sensiblement inférieures» à celles que prévoit le RGPD britannique.

(51) Comme la Commission l'a déjà expliqué, les forums CBPR ne garantissent pas un niveau de protection suffisant pour les données à caractère personnel provenant de l'Union. En particulier, ils ne confèrent pas de droits individuels opposables ([75]). Il est donc particulièrement important de signaler que, même si le Royaume-Uni est un membre associé du forum CBPR, ce dernier ne saurait constituer un mécanisme de transfert valable en vertu de la législation britannique en matière de protection des données. Si cette situation venait à changer, cela compromettrait le niveau de protection actuellement garanti aux données à caractère personnel transférées de l'Union vers le Royaume-Uni. Par conséquent, la Commission continuera de suivre de près l'évolution de la situation à cet égard.

([70]) Disponibles à l'adresse suivante: https://www.legislation.gov.uk/uksi/2022/1213/made.

([71]) Disponibles à l'adresse suivante: https://www.legislation.gov.uk/uksi/2023/1028/made.

([72]) Disponible à l'adresse suivante: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/.

([73]) L'ICO a reçu un grand nombre de demandes de règles d'entreprise contraignantes au Royaume-Uni après le Brexit. De nombreuses règles d'entreprise contraignantes approuvées ne pouvaient plus être utilisées, étant donné que seules les règles d'entreprise contraignantes pour lesquelles l'ICO avait participé au processus d'approbation pouvaient encore être utilisées après le Brexit et que les titulaires de ces règles d'entreprise contraignantes étaient tenus de soumettre à l'ICO une documentation sur leurs règles d'entreprise contraignantes actualisée et mise en conformité avec le RGPD britannique.

([74]) Le forum CBPR (Global Cross-Border Privacy Rules Forum) se compose des États-Unis d'Amérique, du Canada, du Japon, de la République de Corée, des Philippines, de Singapour, de Taïwan et de l'Australie, tandis que Maurice, le Centre financier international de Dubaï et les Bermudes sont des membres associés à l'instar du Royaume-Uni.

([75]) Voir, par exemple, l'analyse comparative effectuée par les autorités de protection des données du G7 sur les éléments essentiels du système de certification du RGPD et du système CBPR, qui a révélé des «différences notables» entre les systèmes, notamment en ce qui concerne «l'opposabilité et les voies de recours, les règles relatives au contrôle indépendant et l'accès des pouvoirs publics». Disponible à l'adresse suivante: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10063165.
Voir considérant 79 de la décision d'exécution (UE) 2019/419 de la Commission du 23 janvier 2019 constatant, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par le Japon en vertu de la loi sur la protection des informations à caractère personnel (JO L 76 du 19.3.2019, p. 1, ELI: http://data.europa.eu/eli/dec_impl/2019/419/oj).
Voir également l'avis 02/2014 du groupe de travail «article 29» concernant des critères de référence pour les exigences applicables aux règles d'entreprise contraignantes à l'intention des autorités nationales compétentes en matière de protection des données dans l'UE, et concernant les règles transfrontalières de protection de la vie privée de l'APEC soumises aux «Accountability Agents» du système CBPR de l'APEC, 6 mars 2014.

2.2.6. *Prise de décision automatisée*

(52) Bien qu'elle conserve plusieurs éléments des règles relatives à la prise de décision automatisée évaluées au considérant 54 de la décision d'exécution (UE) 2021/1772, la loi sur les données (utilisation et accès) a modifié certains aspects de ces règles.

(53) Premièrement, le nouvel article 22B du RGPD britannique interdit de manière générale le traitement portant sur des catégories particulières de données à caractère personnel (définies à l'article 9, paragraphe 1, du RGPD britannique) pour les décisions fondées exclusivement sur un traitement automatisé qui produisent des effets juridiques ou des effets d'une importance similaire pour la personne concernée. Toutefois, trois exceptions à cette interdiction sont prévues: la personne concernée a donné son consentement explicite à ce traitement; ou la décision est nécessaire à la conclusion ou à l'exécution d'un contrat entre le responsable du traitement et la personne concernée; ou le traitement est nécessaire ou autorisé par la loi. Pour ce qui est des deux dernières exceptions, le traitement automatisé doit être nécessaire pour des motifs importants d'intérêt public ([76]). L'interdiction générale ne s'applique pas aux décisions déterminantes fondées sur un traitement automatisé de catégories non particulières de données.

(54) En outre, le nouvel article 22A du RGPD britannique clarifie la définition d'une décision qui est «fondée exclusivement sur un traitement automatisé» en prévoyant qu'il s'agit d'une décision qui ne nécessite aucune intervention humaine significative dans le processus décisionnel. Il est important de noter que les responsables du traitement sont tenus d'évaluer la mesure dans laquelle le profilage contribue à une décision afin de déterminer si l'intervention humaine a été significative. L'article 22A du RGPD britannique précise également qu'une «décision déterminante» est une décision qui produit des effets juridiques pour la personne concernée ou qui l'affecte de manière tout aussi significative ([77]).

(55) Deuxièmement, le nouvel article 22C du RGPD britannique impose aux responsables du traitement de mettre en œuvre des mesures visant à prévoir des garanties pertinentes pour toute décision déterminante fondée entièrement ou partiellement sur des données à caractère personnel et fondée uniquement sur un traitement automatisé (y compris des catégories non particulières de données à caractère personnel). Ces garanties doivent comprendre la fourniture d'informations à la personne concernée sur le processus décisionnel, la possibilité pour la personne concernée de contester la décision et de formuler des observations, et le droit pour la personne concernée d'obtenir une intervention humaine dans le processus décisionnel ([78]).

(56) Enfin, le nouvel article 22D du RGPD britannique investit le secrétaire d'État du pouvoir d'adopter des actes de droit dérivé afin de décrire ce qui constitue, et ce qui ne constitue pas, une intervention humaine significative et quelles décisions sont, et ne sont pas, considérées comme produisant des effets d'une importance similaire sur les personnes concernées. Il permet aussi au secrétaire d'État d'adopter des actes de droit dérivé afin i) d'ajouter de nouvelles garanties; ii) d'imposer des exigences complétant les garanties existantes; et iii) de définir les mesures qui ne satisfont pas aux garanties ([79]). Il est important de noter qu'avant d'adopter des règlements conformément à l'article 22D du RGPD britannique, le secrétaire d'État doit consulter l'ICO ([80]), que les règlements ne peuvent pas modifier l'article 22C du RGPD britannique ([81]) et que les règlements sont soumis à la procédure de résolution positive ([82]), ce qui signifie qu'ils doivent être approuvés par les deux chambres du Parlement britannique avant de pouvoir être adoptés.

(57) Bien que la loi sur les données (utilisation et accès) ait donc modifié le cadre régissant la prise de décision automatisée, il importe de noter que le cadre juridique du Royaume-Uni continue de prévoir que la prise de décision automatisée est soumise aux garanties essentielles exigeant le droit d'obtenir une intervention humaine dans tous les cas de décisions déterminantes fondées exclusivement sur un traitement automatisé, c'est-à-dire pour le traitement de données à caractère personnel sensibles comme non sensibles ([83]). En outre, comme la Commission

([76]) Article 22B du RGPD britannique, tel qu'inséré par l'article 80, paragraphe 1, de la loi sur les données (utilisation et accès).
([77]) Article 22A du RGPD britannique, tel qu'inséré par l'article 80, paragraphe 1, de la loi sur les données (utilisation et accès).
([78]) Article 22C du RGPD britannique, tel qu'inséré par l'article 80, paragraphe 1, de la loi sur les données (utilisation et accès).
([79]) Article 22D du RGPD britannique, tel qu'inséré par l'article 80, paragraphe 1, de la loi sur les données (utilisation et accès). Tout règlement adopté dans le cadre de ces pouvoirs est soumis à la procédure de ratification, assurant ainsi le contrôle parlementaire. Les règlements ne peuvent modifier les exigences énoncées à l'article 22C.
([80]) Article 182, paragraphe 2, de la DPA 2018.
([81]) Article 22D, paragraphe 4, du RGPD britannique.
([82]) Article 22D, paragraphe 5, du RGPD britannique.
([83]) Paragraphe 2 de l'article 22C du RGPD britannique, tel qu'inséré par l'article 80, paragraphe 1, de la loi sur les données (utilisation et accès).

l'a relevé dans de précédentes décisions d'adéquation ([84]), il est peu probable que les règles spécifiques du RGPD britannique relatives à la prise de décision automatisée aient une incidence sur le niveau de protection des données à caractère personnel transférées de l'Union vers le Royaume-Uni. Pour ce qui est des données à caractère personnel qui ont été collectées dans l'Union, toute décision fondée sur un traitement automatisé sera généralement prise par le responsable du traitement de l'Union (qui est en relation directe avec la personne concernée) et relève par conséquent des règles du règlement (UE) 2016/679.

2.3. **Surveillance et contrôle de l'application des règles**

2.3.1. *Surveillance indépendante*

(58) Au Royaume-Uni, une autorité indépendante chargée de veiller à la protection des données continue de surveiller l'application du cadre de protection des données et de le faire respecter, comme indiqué aux considérants 85 à 91 de la décision d'exécution (UE) 2021/1772. La loi sur les données (utilisation et accès) améliore la structure de gouvernance de cette autorité en créant une personne morale constituée en société, l'*Information Commission* (ci-après la «commission de l'information»), qui remplacera l'ICO, lequel était structuré comme une personne morale individuelle.

(59) Plus précisément, les mesures de gouvernance énoncées dans la loi sur les données (utilisation et accès), une fois mises en œuvre, supprimeront le bureau du commissaire à l'information et transféreront les fonctions, le personnel et les biens de l'ICO à la nouvelle entité, la commission de l'information. La commission de l'information est composée de membres exécutifs et non exécutifs ([85]). En outre, en vertu de la loi, le commissaire à l'information se voit confier le poste de président de la commission de l'information, qui est l'un des membres non exécutifs ([86]). La loi sur les données (utilisation et accès) prévoit en outre que, dans la mesure où cela est approprié en raison du transfert de fonctions, les références au commissaire à l'information dans tous les actes législatifs ou autres documents (lorsqu'ils sont adoptés ou émis) doivent être lues comme des références à la commission de l'information. Dans l'exercice de ses fonctions, la commission peut instituer des comités et déléguer certaines fonctions à un membre, à un employé ou à l'un de ses comités ([87]) et peut prendre des dispositions concernant ses propres procédures et celles que doivent suivre les comités, y compris pour ce qui est du quorum et la prise de décisions à la majorité. Ces procédures doivent être rendues publiques ([88]).

(60) Il convient de noter que l'indépendance de la commission de l'information est soumise aux mêmes garanties, y compris en ce qui concerne les règles relatives à la nomination et à la révocation du président, que celles qui font l'objet d'une appréciation aux considérants 87 à 90 de la décision d'exécution (UE) 2021/1772 ([89]). Des garanties similaires s'appliquent en ce qui concerne les autres membres non exécutifs de la commission de l'information. En particulier, le président de la commission de l'information est nommé par Sa Majesté sur recommandation du secrétaire d'État. Il est sélectionné sur la base de ses compétences à l'issue d'un concours équitable et ouvert ([90]). Les autres membres non exécutifs sont nommés par le secrétaire d'État, après consultation du président. Les candidats ne peuvent être recommandés en vue de leur nomination ou ne peuvent être nommés que s'ils sont sélectionnés sur la base de leurs compétences à l'issue d'un concours équitable et ouvert et que si le secrétaire d'État estime qu'ils ne se trouvent pas dans une situation de conflit d'intérêts ([91]). Les membres exécutifs sont des membres de la commission de l'information soumis aux règles et conditions fixées par les membres non exécutifs ([92]). Le directeur est nommé par le président et les autres membres non exécutifs après consultation du secrétaire d'État. Les membres exécutifs sont également nommés sur la base de leurs compétences à l'issue d'un concours équitable et ouvert ([93]).

(61) Le président ne peut être démis de ses fonctions que par Sa Majesté sur requête des deux chambres du Parlement et uniquement si le secrétaire d'État a présenté à la chambre un rapport dont il ressort que le président a commis une faute grave, qu'il se trouve dans une situation de conflit d'intérêts, qu'il ne s'est pas conformé aux exigences

([84]) Voir, par exemple, considérant 94 de la décision d'exécution (UE) 2019/419 et considérant 81 de la décision d'exécution (UE) 2022/254 de la Commission du 17 décembre 2021 constatant, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la République de Corée en vertu de la loi sur la protection des informations à caractère personnel (JO L 44 du 24.2.2022, p. 1, ELI: http://data.europa.eu/eli/dec_impl/2022/254/oj).
([85]) Point 3.1 de l'annexe 12A de la DPA 2018.
([86]) Articles 117, 118, 119 et 120, lus en combinaison avec l'annexe 14 de la loi sur les données (utilisation et accès).
([87]) Points 13 et 14 de l'annexe 12A de la DPA 2018.
([88]) Point 16 de l'annexe 12A de la DPA 2018.
([89]) Article 52 du RGPD britannique et annexe 12A de la DPA 2018, telle qu'ajoutée par l'article 114A du projet de loi sur les données (utilisation et accès).
([90]) Points 5.1 et 3.2 de l'annexe 12A de la DPA 2018.
([91]) Points 3.2, 5 et 6 de l'annexe 12A de la DPA 2018.
([92]) Point 11 de l'annexe 12A de la DPA 2018.
([93]) Point 5.2 de l'annexe 12A de la DPA 2018.

spécifiques en matière d'information quant à l'existence d'éventuels conflits d'intérêts ou qu'il n'est pas à même d'accomplir les fonctions inhérentes à la présidence, qu'il se trouve dans l'incapacité de les accomplir ou qu'il n'est pas disposé à les accomplir ([94]). Les membres non exécutifs ne peuvent être démis de leurs fonctions par le secrétaire d'État que si celui-ci estime que les conditions spécifiques énoncées dans la législation sont réunies. Parmi ces conditions figurent l'existence d'un conflit d'intérêts, le fait d'avoir commis une faute grave ou le fait de ne pas être à même d'accomplir leurs fonctions, de ne pas être disposés à les accomplir ou de se trouver dans l'incapacité de les accomplir. En termes de garanties supplémentaires, le secrétaire d'État est tenu de publier la décision de révocation et de fournir au membre un exposé des motifs de sa révocation ([95]).

(62) Le rôle principal de la commission de l'information restera le suivi et l'application du cadre de protection des données au Royaume-Uni «afin de protéger les libertés et droits fondamentaux» des personnes physiques ([96]). En ce qui concerne la fonction de la commission de l'information consistant à garantir un niveau approprié de protection des données à caractère personnel, la loi sur les données (utilisation et accès) exige spécifiquement que la commission de l'information tienne compte des intérêts des personnes concernées, des responsables du traitement et des tiers, ainsi que de l'intérêt public général, et qu'elle promeuve la confiance du public dans le traitement des données à caractère personnel ([97]). Ces objectifs sont également mentionnés au considérant 7 du règlement (UE) 2016/679.

(63) En outre, la loi sur les données (utilisation et accès) précise que la commission de l'information tient compte de l'opportunité d'encourager l'innovation et la concurrence, de l'importance de la prévention et de la détection des infractions pénales ainsi que des enquêtes et des poursuites en la matière, de la nécessité de préserver la sécurité publique et la sécurité nationale, de même que des besoins spécifiques liés à la protection des enfants dans l'exercice de sa fonction au titre de la législation sur la protection des données ([98]). La législation de l'Union en matière de protection des données reconnaît également la nécessité de mettre en balance la protection des données à caractère personnel et plusieurs autres droits fondamentaux et objectifs, tels que le progrès économique et social, la sécurité et la justice et la liberté d'entreprise ([99]).

2.3.2. *Contrôle de l'application des règles, y compris les sanctions*

(64) Les pouvoirs et les tâches de la commission de l'information continuent de correspondre aux pouvoirs et aux tâches qui incombent aux autorités contrôlant la protection des données dans les États membres en vertu des articles pertinents du règlement (UE) 2016/679 ([100]), comme indiqué aux considérants 91 à 95 de la décision d'exécution (UE) 2021/1772.

(65) La loi sur les données (utilisation et accès) a apporté certaines précisions concernant l'exercice de certains de ces pouvoirs.

(66) D'une part, la loi sur les données (utilisation et accès) précise que la commission peut exiger des «documents» et des «informations» spécifiques lorsqu'elle utilise son pouvoir l'habilitant à émettre des avis d'information ([101]). D'autre part, la loi sur les données (utilisation et accès) introduit deux nouveaux pouvoirs d'enquête pour la commission de l'information, soit un nouveau pouvoir lui permettant d'exiger un signalement ([102]) et un nouveau pouvoir lui permettant de délivrer des «avis d'entretien» aux responsables du traitement en cas de violation présumée du RGPD britannique ou de la DPA 2018 ([103]).

([94]) Points 7.6 et 7.7 de l'annexe 12A de la DPA 2018.
([95]) Points 9.6, 7, 8 et 9 de l'annexe 12A de la DPA 2018.
([96]) Article 51 du RGPD britannique.
([97]) Article 91 de la loi sur les données (utilisation et accès), insérant un article 120A à la DPA 2018.
([98]) Article 91 de la loi sur les données (utilisation et accès), ajoutant un article 120B à la DPA 2018. La loi sur les données (utilisation et accès) ajoute en outre à la DPA 2018 un nouvel article (l'article 120C), qui impose à la commission de l'information d'élaborer et de publier une stratégie reflétant notamment la manière dont elle examinera les questions susmentionnées et l'opportunité d'encourager la croissance économique dans l'exercice de ses fonctions réglementaires.
([99]) Voir, en particulier, les considérants 2 et 4 et l'article 23 du règlement (UE) 2016/679.
([100]) Articles 57 et 58 du RGPD britannique.
([101]) Article 97 de la loi sur les données (utilisation et accès), modifiant l'article 142 de la DPA 2018. Les considérations relatives à l'incidence de la technologie et au rôle de la protection des données pour susciter la confiance dans l'économie numérique font partie des activités des autorités de régulation de la protection des données tant au Royaume-Uni que dans l'Union. Voir, par exemple, le rapport annuel 2024 du comité européen de la protection des données, p. 12: «Le comité européen de la protection des données est un organe dynamique et collaboratif qui joue un rôle central pour l'application cohérente de la législation en matière de protection des données dans toute l'Europe. De mon point de vue, en tant que vice-président, je le considère comme un gardien des droits des personnes au respect de leur vie privée, qui garantit un équilibre délicat avec les besoins en matière d'innovation et de croissance économique.»
([102]) Article 98 de la loi sur les données (utilisation et accès), modifiant l'article 146 de la DPA 2018.
([103]) Article 100 de la loi sur les données (utilisation et accès), insérant un article 148A dans la DPA 2018.

(67) En ce qui concerne l'exercice de ces pouvoirs par la commission de l'information, depuis l'entrée en vigueur de la décision d'exécution (UE) 2021/1772, le commissaire à l'information a traité environ 40 000 réclamations de personnes concernées par an, ce qui est proche du nombre de réclamations traitées lorsque le Royaume-Uni faisait toujours partie de l'Union et appliquait encore le règlement (UE) 2016/679 ([104]). L'ICO a également mené des enquêtes d'office portant sur un large éventail de questions sectorielles et de conformité, y compris les droits des personnes concernées ([105]).

(68) En ce qui concerne les mesures d'exécution, depuis l'entrée en vigueur de la décision d'exécution (UE) 2021/1772, le commissaire a émis 120 rappels à l'ordre, 32 avis d'information, 3 avis d'évaluation, 12 avis d'exécution et 2 avertissements et a infligé 12 amendes ([106]). Il a notamment imposé plusieurs sanctions pécuniaires importantes au titre du RGPD britannique et de la DPA 2018. Par exemple, en avril 2023, le commissaire à l'information a infligé une amende de 12,7 millions de livres sterling (GBP) à une plateforme de médias sociaux pour utilisation abusive de données concernant des enfants ([107]). En mars 2025, il a infligé une amende de 3,07 millions de GBP à une société de logiciels pour des manquements en matière de sécurité ayant compromis les informations à caractère personnel de plus de 70 000 personnes ([108]). Très récemment, en juin 2025, il a infligé une amende de 2,31 millions de GBP à une entreprise de tests génétiques pour n'avoir pas mis en œuvre les mesures de sécurité appropriées pour protéger les informations à caractère personnel des utilisateurs britanniques à la suite d'une cyberattaque à grande échelle menée en 2023 ([109]).

(69) Depuis l'adoption de la décision d'exécution (UE) 2021/1772, le Bureau du commissaire à l'information a également élaboré et publié un nombre important de lignes directrices, d'avis et d'autres documents d'orientation clarifiant l'application des règles en matière de protection des données dans des domaines importants, tels que la reconnaissance faciale, l'équité en matière d'intelligence artificielle, les données concernant les enfants, le marketing direct, la vidéosurveillance, le droit d'accès et la transparence en matière de soins de santé et d'aide sociale, à l'intention de différents publics, parmi lesquels les petites et moyennes entreprises, des entités spécifiques comme les écoles, les crèches ou les autorités publiques de petite taille, ou encore les entreprises en général, le grand public et les personnes concernées ([110]).

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

3.1. Cadre juridique général

(70) Le Royaume-Uni est toujours membre du Conseil de l'Europe et continue d'adhérer à la convention européenne des droits de l'homme et d'être soumis à la compétence de la Cour européenne des droits de l'homme. Il reste donc soumis aux obligations consacrées par le droit international qui sont décrites aux considérants 116 à 119 de la décision d'exécution (UE) 2021/1772, qui encadrent au Royaume-Uni, en tant que partie à la CEDH, le système d'accès des pouvoirs publics aux données à caractère personnel sur la base de principes, de garanties et de droits individuels identiques à ceux qui s'appliquent aux 27 États membres et qui se reflètent, dans une large mesure, dans la jurisprudence pertinente de la Cour de justice de l'Union européenne.

(71) La DPA 2018 continue de prévoir des garanties et des droits spécifiques en matière de protection des données dans le cadre du traitement des données par les autorités publiques au Royaume-Uni, notamment les autorités répressives et les agences de sécurité nationale, comme indiqué aux considérants 121 à 132 de la décision d'exécution (UE) 2021/1772. La loi sur les données (utilisation et accès) n'a apporté que des modifications limitées et ciblées aux parties de la DPA 2018 qui énoncent les règles relatives au traitement des données à caractère personnel à des fins répressives (partie 3 de la DPA 2018) et à des fins de sécurité nationale (partie 4 de la DPA 2018).

([104]) Rapports annuels du commissaire à l'information pour les périodes 2021-2022, 2022-2023 et 2023-2024. Voir, également, le considérant 96 de la décision d'exécution (UE) 2021/1772.

([105]) Rapport annuel du commissaire à l'information pour la période 2023-2024, p. 41.

([106]) Rapports annuels du commissaire à l'information pour les périodes 2021-2022, 2022-2023 et 2023-2024.

([107]) Pour de plus amples informations sur ces mesures d'exécution et d'autres, veuillez consulter le site web de l'ICO à l'adresse suivante: https://ico.org.uk/action-weve-taken/enforcement/.

([108]) De plus amples informations sont disponibles à l'adresse suivante: https://ico.org.uk/action-weve-taken/enforcement/2025/03/advanced-computer-software-group-limited/.

([109]) De plus amples informations sont disponibles à l'adresse suivante: https://ico.org.uk/action-weve-taken/enforcement/2025/06/23andme/.

([110]) Disponibles à l'adresse suivante: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/.

(72) En ce qui concerne le traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, la partie 3 de la DPA 2018 continue de prévoir des principes, des droits et des obligations semblables à ceux qui sont énoncés dans la directive (UE) 2016/680 ([111]).

(73) En particulier, à la même date que pour la présente décision, la Commission a adopté une décision en vertu de l'article 36, paragraphe 3, de la directive (UE) 2016/680, constatant que le régime de protection des données applicable au traitement des données par les autorités répressives britanniques à des fins répressives continue d'assurer un niveau de protection essentiellement équivalent à celui garanti par la directive (UE) 2016/680.

(74) La loi sur les données (utilisation et accès) a modifié et consolidé les exemptions existantes accordées conformément à la partie 3 de la DPA 2018 aux autorités compétentes à des fins de sécurité nationale. L'exemption en matière de sécurité nationale permet aux autorités compétentes de ne pas appliquer certaines dispositions de la partie 3 de la DPA 2018 si une dérogation à celles-ci est nécessaire aux fins de la sauvegarde de la sécurité nationale ([112]). Il reflète les exemptions en matière de sécurité nationale prévues pour le traitement des données à caractère personnel en vertu du RGPD britannique (article 26 de la DPA 2018) et de la partie 4 de la DPA 2018 (article 110 de la DPA 2018).

(75) L'exemption liée à la sécurité nationale est soumise aux mêmes limitations et garanties que les exemptions prévues par le RGPD britannique et la partie 4 de la DPA 2018, telles qu'analysées aux considérants 64 à 67 et 126 de la décision d'exécution (UE) 2021/1772. En particulier, l'exemption ne peut être appliquée que dans la mesure où elle est nécessaire pour garantir la sécurité nationale. Il ne s'agit pas d'une exemption générale. Elle doit être examinée et invoquée par le responsable du traitement au cas par cas ([113]). De plus, toute application de l'exemption doit être conforme aux normes relatives aux droits de l'homme (fondées sur la loi de 1998 sur les droits de l'homme et sur la Convention européenne des droits de l'homme), selon lesquelles toute ingérence dans l'exercice du droit au respect de la vie privée devrait, dans une société démocratique, constituer une mesure nécessaire et proportionnée ([114]). Cela est également confirmé dans les orientations de l'ICO sur l'application des dérogations en matière de sécurité nationale ([115]).

(76) En outre, sur la base des modifications introduites par la loi sur les données (utilisation et accès) ([116]), une activité de traitement spécifique menée par les autorités compétentes à des fins répressives peut également être régie par les dispositions de la partie 4 de la DPA 2018, qui ne s'applique normalement qu'au traitement des données par les agences de sécurité nationale.

([111]) L'article 69 de la loi sur les données (utilisation et accès) insère dans la DPA 2018, en tant que nouvel article 33, paragraphe 1A, et que nouvel article 40A, la définition du consentement et les conditions de recours au consentement qui sont prévues à l'article 4, paragraphe 11, et à l'article 7 du RGPD britannique [qui reflètent les dispositions correspondantes du règlement (UE) 2016/679] et clarifie de la sorte la notion de consentement et les conditions dans lesquelles le consentement peut servir de base juridique pour le traitement des données à caractère personnel par les autorités compétentes à des fins répressives. En outre, l'article 71, paragraphes 7 et 8, de la loi sur les données (utilisation et accès) clarifie quelque peu le libellé de l'article 36, paragraphe 1, de la DPA 2018. Enfin, les modifications apportées au RGPD britannique par la loi sur les données (utilisation et accès) qui sont décrites à l'article 2 se reflètent aussi, le cas échéant, dans la partie 3 de la DPA 2018; voir, par exemple, l'article 74, paragraphes 2 à 5, concernant le traitement des données à caractère sensible, l'article 76, paragraphes 4 à 6, concernant les délais de réponse aux demandes des personnes concernées, l'article 78, paragraphes 2 et 3, concernant les recherches menées en réponse aux demandes des personnes concernées, ainsi que l'article 80, paragraphes 3 à 5, concernant la prise de décision automatisée.

([112]) Article 78A, paragraphe 1, de la loi DPA 2018, tel qu'inséré par l'article 88 de la loi sur les données (utilisation et accès). Conformément à l'article 78A, paragraphes 2 à 4, de la DPA 2018, l'exemption permet de ne pas appliquer les principes de protection des données (à l'exception du principe de licéité et des conditions et garanties applicables au traitement des données sensibles), les droits individuels, les obligations des responsables du traitement et des sous-traitants en ce qui concerne les violations de données, certaines parties des règles relatives aux transferts de données à l'échelle internationale et certains pouvoirs conféré au commissaire à l'information en vue de la réalisation d'inspections et de l'adoption de mesures coercitives.

([113]) Voir l'arrêt dans l'affaire Baker/Secretary of State for the Home Department [2001] UKIT NSA2 («Baker/Secretary of State»).

([114]) Voir également l'arrêt dans l'affaire Guriev/Community Safety Development (UK) Ltd [2016] EWHC 643 (QB), point 45, et l'arrêt dans l'affaire Lin/Commissioner of the Police for the Metropolis [2015] EWHC 2484 (QB), point 80.

([115]) Voir les orientations de l'ICO sur l'exception en matière de sécurité et de défense nationales, disponibles à l'adresse suivante: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/national-security-and-defence-exemption-a-guide.

([116]) Articles 89 et 90 de la loi sur les données (utilisation et accès).

(77) Si le régime de protection des données pour le traitement à des fins de sécurité nationale est donc, dans certaines situations, étendu également au traitement des données par les autorités répressives, ce n'est le cas que dans des circonstances spécifiques et sous réserve de conditions et de garanties strictes, c'est-à-dire i) si une autorité compétente est désignée comme une «autorité compétente qualifiée» dans des règlements adoptés par le secrétaire d'État qui nécessitent l'approbation du Parlement ([117]) et ii) si le secrétaire d'État désigne, par un avis, une activité de traitement spécifique effectuée par l'autorité compétente qualifiée. Il est important de noter qu'une telle désignation ne peut avoir lieu que si le secrétaire d'État considère que la désignation de l'activité de traitement est nécessaire pour garantir la sécurité nationale, c'est-à-dire lorsqu'une autorité répressive agit à des fins de sécurité nationale et que l'activité de traitement est effectuée par l'autorité compétente qualifiée en sa qualité de responsable conjoint du traitement avec au moins un service de renseignement ([118]). À titre de garanties supplémentaires, le secrétaire d'État doit consulter le commissaire avant d'émettre un avis de désignation ([119]); le texte de l'avis doit en principe être publié ([120]) et une personne directement concernée par un avis de désignation peut demander un contrôle juridictionnel ([121]). Par conséquent, cette modification vise essentiellement à préciser que, lorsque les autorités britanniques ont des compétences à la fois à des fins répressives et à des fins de sécurité nationale et traitent les données dans le cadre de cette dernière finalité, le régime de protection des données pour les agences de sécurité nationale peut s'appliquer.

(78) La partie 4 de la DPA 2018 régit le traitement des données par les services de renseignement britanniques. Elle continue d'énoncer les grands principes relatifs à la protection des données, d'imposer des conditions au traitement de catégories particulières de données, d'établir les droits des personnes concernées, d'exiger la protection des données dès la conception et de réglementer les transferts de données à caractère personnel, comme indiqué aux considérants 125 à 132 de la décision d'exécution (UE) 2021/1772.

(79) Les modifications apportées à ce régime par la loi sur les données (utilisation et accès) sont limitées. En ce qui concerne le droit d'accès des personnes concernées prévu à l'article 94 de la DPA 2018, la loi sur les données (utilisation et accès) insère un nouveau paragraphe (le paragraphe 2A) afin de préciser que la personne concernée n'a droit aux informations pertinentes que dans la mesure où le responsable du traitement est à même de les lui fournir sur la base d'une recherche raisonnable et proportionnée ([122]). Comme expliqué au considérant 35, cette modification encadre le droit d'accès par des normes juridiques établies, qui tiennent également compte des intérêts de la personne concernée. Même si, dans le domaine de la prise de décision automatisée, il est toujours interdit aux responsables du traitement de prendre une décision qui affecte de manière significative une personne concernée qui soit fondée exclusivement sur un traitement automatisé des données à caractère personnel la concernant, à moins qu'une telle décision ne soit nécessaire ou autorisée par la loi, que la personne concernée ait donné son consentement à ce que la décision soit prise sur cette base ou que la décision soit prise dans le cadre d'un contrat ([123]), la loi sur les données (utilisation et accès) insère dans la partie 4 de la DPA 2018 ([124]), pour la notion de «décision fondée exclusivement sur un traitement automatisé», la même définition que celle qui figure à l'article 22A du RGPD britannique et qui a été analysée au considérant 53 de la présente décision.

3.2. Évolutions pertinentes concernant l'accès aux données et l'utilisation de celles-ci par les autorités publiques du Royaume-Uni à des fins répressives

(80) Le droit du Royaume-Uni continue d'imposer des limitations importantes à l'accès aux données à caractère personnel et à l'utilisation de celles-ci à des fins répressives, et continue également de prévoir des mécanismes de surveillance et de recours dans ce domaine, comme indiqué aux considérants 134 à 174 de la décision d'exécution (UE) 2021/1772.

([117]) Article 82, paragraphes A1, 2A et 4, de la DPA 2018, tels qu'insérés par l'article 89, paragraphe 2, de la loi sur les données (utilisation et accès).

([118]) Article 82A, paragraphes 1 et 2, tels qu'inséré par l'article 89, paragraphe 3, de la loi sur les données (utilisation et accès). À titre de garanties supplémentaires, le secrétaire d'État doit consulter le commissaire avant d'émettre un avis de désignation (voir le paragraphe 8 du nouvel article 82A de la DPA 2018); le texte de l'avis doit en principe être publié (voir le paragraphe 1 du nouvel article 82D), sous réserve des exceptions énoncées dans le paragraphe 3 du nouvel article 82D de la DPA 2018, et une personne directement concernée par un avis de désignation peut demander un contrôle juridictionnel (voir le nouvel article 82E de la DPA 2018).

([119]) Article 82A, paragraphe 8, de la DPA 2018.

([120]) Article 82D, paragraphe 1, sous réserve des exemptions prévues au nouvel article 82D, paragraphe 3, de la DPA 2018.

([121]) Article 82E de la DPA 2018.

([122]) Article 78, paragraphe 4, de la loi sur les données (utilisation et accès).

([123]) Article 96 de la DPA 2018.

([124]) En vertu du nouveau paragraphe 4 de l'article 96 de la DPA 2018, une décision est fondée sur un traitement entièrement automatisé si le processus décisionnel ne prévoit pas la possibilité pour un être humain d'accepter, de rejeter ou d'influencer la décision. Article 80, paragraphe 4, point c), de la loi sur les données (utilisation et accès).

3.2.1. *Bases juridiques et limitations/garanties applicables*

(81) La collecte des données à caractère personnel auprès des opérateurs économiques au Royaume-Uni à des fins répressives est encore autorisée dans le cadre juridique du Royaume-Uni sur la base de mandats de perquisition et d'injonctions de production, sous réserve des conditions et des garanties décrites aux considérants 135 à 138 de la décision d'exécution (UE) 2021/1772.

(82) En outre, la loi de 2023 sur la sécurité nationale ([125]) qui vise à lutter contre les menaces que posent pour la sécurité nationale l'espionnage, le sabotage et les personnes agissant pour le compte de puissances étrangères, a investi la police britannique de nouveaux pouvoirs d'entrée, de perquisition et de saisie, y compris la possibilité d'obtenir des données à caractère personnel, lorsqu'il existe des motifs raisonnables de soupçonner que la mesure permettra d'obtenir des éléments susceptibles de prouver que l'une des infractions les plus graves ou l'une des menaces les plus graves posée par une puissance étrangère, selon la loi de 2023 sur la sécurité nationale, a été commise ou est sur le point d'être commise ([126]). Ces pouvoirs sont soumis à des conditions et garanties semblables aux conditions et garanties analysées dans la décision d'exécution (UE) 2021/1772 en ce qui concerne les pouvoirs existant à l'époque. En particulier, leur utilisation doit être autorisée au moyen d'un mandat, d'une injonction de production ou d'une injonction d'explication délivré par une instance judiciaire indépendante, en principe sur demande de l'officier/de l'enquêteur ([127]). Des protections spécifiques existent pour les documents confidentiels, tels que les éléments journalistiques et les éléments couverts par le secret professionnel ([128]). De même, les injonctions de divulgation ([129]), les injonctions d'information sur la clientèle ([130]) et les injonctions de contrôle des comptes ([131]), également créées par la loi de 2023 sur la sécurité nationale, doivent être délivrées par un juge à la demande d'un officier compétent et sont soumises à des conditions et garanties spécifiques. L'injonction doit notamment être demandée à l'égard d'une personne déterminée, aux fins d'une enquête sur une menace posée par une puissance étrangère, doit viser à renforcer l'efficacité de l'enquête et ne doit pas être utilisée pour obtenir des informations légalement protégées ou par ailleurs exclues, telles que les éléments journalistiques et certains dossiers médicaux ([132]).

(83) Comme expliqué aux considérants 139 à 141 de la décision d'exécution (UE) 2021/1772, dans le cadre juridique du Royaume-Uni, des autorités répressives spécifiques, comme, par exemple, l'Agence nationale de lutte contre la criminalité ou le Metropolitan Police Service, peuvent également exercer des pouvoirs d'enquête ciblés au titre de la loi de 2016 sur les pouvoirs d'enquête (IPA 2016) ([133]) aux fins de la prévention ou de la détection des infractions graves. Ces autorités répressives peuvent s'appuyer sur des pouvoirs d'enquête spécifiques, à savoir les interceptions ciblées (partie 2 de l'IPA 2016), l'acquisition de données de communication (partie 3 de l'IPA 2016) et le piratage ciblé d'équipements (partie 5 de l'IPA 2016). Lorsque des avis de conservation sont émis par le secrétaire d'État en vertu de la partie 4 de l'IPA 2016, les services répressifs peuvent également en bénéficier en accédant aux données relatives aux communications qui sont conservées au moyen de pouvoirs d'acquisition de données de communications conférés en vertu de la partie 3 de l'IPA 2016.

([125]) Disponible à l'adresse suivante: https://www.legislation.gov.uk/ukpga/2023/32/contents/enacted.

([126]) Annexe 2 de la loi de 2023 sur la sécurité nationale. Les infractions pertinentes au titre de la loi de 2023 sur la sécurité nationale sont, par exemple, l'obtention ou la divulgation d'informations protégées (article 1er), l'obtention ou la divulgation de secrets d'affaires (article 3), l'assistance à un service de renseignement étranger (article 4), la réalisation d'un acte de sabotage (article 12) ou l'exécution d'une activité interdite spécifique pour le compte d'une puissance étrangère à des fins d'ingérence (article 13).

([127]) Voir points 2.1, 3.1, 4.1 et 10.1 de l'annexe 2 de la loi de 2023 sur la sécurité nationale.

([128]) Voir les points 2.4.b), 3.4.b) et c), 4.4.b) et c), ainsi que 10.1 de l'annexe 2 de la loi de 2023 sur la sécurité nationale.

([129]) Par une injonction de divulgation au titre de l'annexe 3 de la loi de 2023 sur la sécurité nationale, un officier peut ordonner à une personne de fournir des informations, de produire des documents et/ou de répondre à des questions pertinentes pour une enquête visant à identifier des biens liés à une menace posée par une puissance étrangère, y compris le mouvement ou l'utilisation des biens.

([130]) Par une injonction d'information sur la clientèle au titre de l'annexe 4 de la loi de 2023 sur la sécurité nationale, un officier peut ordonner à un établissement financier de fournir toute information sur sa clientèle en rapport avec une personne déterminée.

([131]) Par une injonction de contrôle des comptes au titre de l'annexe 5, un officier peut ordonner à un établissement financier de fournir, pour la période et selon les modalités précisées dans l'injonction, les informations spécifiées dans celle-ci, couvrant une période maximale de 90 jours.

([132]) Annexe 3, point 2.1, annexe 4, point 1, et annexe 5, point 1, de la loi de 2023 sur la sécurité nationale.

([133]) La loi de 2016 sur les pouvoirs d'enquête (voir: https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted) a remplacé différentes lois relatives à l'interception de communications, au piratage d'équipements et à l'acquisition de données de communication, en particulier la partie I de la RIPA 2000 qui a institué le précédent cadre législatif général relatif à l'utilisation des pouvoirs d'enquête par les autorités répressives et les agences de sécurité nationale.

(84) Depuis l'adoption de la décision d'exécution (UE) 2021/1772, l'IPA 2016, avec la loi de 2000 portant réglementation des pouvoirs d'enquête (RIPA 2000) pour l'Angleterre, le pays de Galles et l'Irlande du Nord et la loi écossaise de 2000 sur la réglementation des pouvoirs d'enquête pour l'Écosse, continue de constituer la base juridique de ces pouvoirs et de définir les limitations et les garanties relatives à l'exercice de ces pouvoirs, comme indiqué dans la décision d'exécution (UE) 2021/1772. Il convient de noter que le cadre juridique continue d'exiger que, pour exercer ces pouvoirs, les autorités obtiennent un mandat ([134]) délivré par une autorité compétente ([135]) et approuvé par un commissaire judiciaire indépendant ([136]) (procédure dite «de double verrouillage»). L'obtention de ce mandat reste soumise à un critère de nécessité et de proportionnalité ([137]).

(85) Dans le même temps, depuis l'adoption de la décision d'exécution (UE) 2021/1772, la loi de 2024 sur les pouvoirs d'enquête (modification), à laquelle l'assentiment royal a été accordé en avril 2024, a modifié certains éléments spécifiques de l'IPA 2016 ([138]). Dans la mesure où ces modifications et d'autres évolutions pertinentes concernent les conditions, les limitations et les garanties relatives à l'utilisation des pouvoirs d'enquête spécifiques susmentionnés par les autorités publiques britanniques à des fins répressives qui ont été évaluées aux considérants 177 à 215 de la décision d'exécution (UE) 2021/1772, elles sont analysées ci-après. En ce qui concerne les éléments du cadre du Royaume-Uni qui n'ont pas été modifiés par la loi susmentionnée ou qui n'ont pas été affectés par d'autres évolutions pertinentes, l'analyse effectuée dans la décision d'exécution (UE) 2021/1772 reste valable.

(86) En ce qui concerne l'acquisition et la conservation ciblées de données de communication ([139]), les conditions et les garanties régissant ces pouvoirs qui ont été évaluées dans la décision d'exécution (UE) 2021/1772 restent en place. La loi de 2024 sur les pouvoirs d'enquête (modification) a clarifié les garanties existantes en insérant à l'article 11 de l'IPA 2016 (qui crée une infraction pour l'obtention illicite de données de communication auprès d'un opérateur de télécommunications) une liste d'exemples de ce que l'on entend par «habilitation légale» aux fins de cette disposition ([140]). En outre, la loi de 2024 sur les pouvoirs d'enquête (modification) a encore clarifié la définition des données de communication figurant à l'article 261 de l'IPA 2016 en précisant explicitement que les données relatives aux abonnés sont considérées comme des données de communication ([141]).

([134]) La partie 2, chapitre 2, de l'IPA 2016 prévoit un nombre limité de cas dans lesquels les interceptions peuvent être effectuées sans mandat. Il s'agit notamment: des interceptions moyennant le consentement de l'expéditeur ou du destinataire, des interceptions à des fins administratives ou d'application des règles, des interceptions ayant lieu dans certains établissements (prisons, hôpitaux psychiatriques et centres de détention de l'immigration), ainsi que des interceptions réalisées conformément à un accord international en vigueur.

([135]) Dans la plupart des cas, le secrétaire d'État est l'autorité qui délivre les mandats au titre de l'IPA 2016, tandis que les ministres écossais sont habilités à délivrer des mandats d'interception ciblée, d'entraide judiciaire et de piratage ciblé d'équipements lorsque les personnes ou les locaux visés par l'interception et les équipements concernés par l'interférence sont situés en Écosse (voir articles 22 et 103 de l'IPA 2016). En cas de piratage ciblé d'équipements, le chef des forces de police (tel qu'il est décrit à l'annexe 6, parties 1 et 2, de l'IPA 2016) peut délivrer le mandat dans les conditions prévues à l'article 106 de l'IPA 2016.

([136]) Les commissaires judiciaires assistent le commissaire aux pouvoirs d'enquête (Investigatory Powers Commissioner, IPC), un organe indépendant qui exerce des fonctions de surveillance de l'utilisation des pouvoirs d'enquête par les services de renseignement.

([137]) Voir, en particulier, articles 19 et 23 de l'IPA 2016.

([138]) Disponible à l'adresse suivante: https://www.legislation.gov.uk/ukpga/2024/9/contents/2025-04-25.

([139]) Le terme «données de communication» recouvre le «qui», le «quand», le «où» et le «comment» d'une communication, mais pas son contenu, c'est-à-dire ce qui a été dit ou écrit. Il peut s'agir, par exemple, de l'heure et de la durée d'une communication, du numéro ou de l'adresse électronique de l'expéditeur et du destinataire, et parfois de la localisation des appareils à partir desquels la télécommunication a été effectuée (voir article 261, paragraphe 5, de l'IPA 2016). En vertu de l'IPA 2016, le secrétaire d'État peut obliger les opérateurs de télécommunications à conserver des données de communication en vue d'un accès ciblé à celles-ci par diverses autorités publiques, notamment les autorités répressives et les agences de renseignement. La partie 4 de l'IPA 2016 régit la conservation des données de communication, tandis que la partie 3 régit l'acquisition ciblée de données de communication. Les parties 3 et 4 de l'IPA 2016 définissent également des limitations spécifiques à l'utilisation de ces pouvoirs et prévoient des garanties spécifiques.

([140]) Par exemple, lorsque la personne compétente obtient les données de communication dans l'exercice d'un pouvoir réglementaire de l'autorité publique concernée ou lorsque les données de communication sont obtenues conformément à une décision de justice ou à une autre autorisation judiciaire. Paragraphe 3A de l'article 11 de l'IPA 2016, tel qu'inséré par l'article 12, point 3, de la loi de 2024 sur les pouvoirs d'enquête (modification).

([141]) Paragraphes 5A et 5B de l'article 261, tels qu'insérés par la section 13, point 3, de la loi de 2024 sur les pouvoirs d'enquête (modification).

(87) L'émission des avis ordonnant la conservation de données de communication ([142]) reste soumise aux limitations et garanties décrites aux considérants 208 et 209 de la décision d'exécution (UE) 2021/1772, en particulier les exigences de nécessité et de proportionnalité, et l'approbation par un commissaire judiciaire indépendant. Bien que la loi de 2024 sur les pouvoirs d'enquête (modification) ait introduit la possibilité de renouveler ces avis, tout renouvellement est soumis aux mêmes conditions de nécessité et de proportionnalité et à l'approbation du commissaire judiciaire ([143]).

(88) En ce qui concerne les données relatives aux communications, la loi de 2024 sur les pouvoirs d'enquête (modification) a également modifié la définition des opérateurs de télécommunications, c'est-à-dire les destinataires potentiels d'un avis de conservation. Cette définition inclut désormais toute personne «contrôlant ou fournissant un système de télécommunications qui i) n'est pas (totalement ou partiellement) établi au Royaume-Uni ou contrôlé depuis le Royaume-Uni et qui ii) est utilisé par une autre personne pour offrir ou fournir un service de télécommunications à des personnes au Royaume-Uni» ([144]). Il convient de noter que la définition modifiée continue de prévoir un lien étroit avec le marché du Royaume-Uni. La modification apportée permet donc de préciser que les grandes entreprises s'appuyant sur une structure complexe sont intégralement couvertes par l'IPA 2016, sans que le champ d'application de la définition soit étendu aux fournisseurs de services de télécommunications qui ne s'adressent pas à des personnes au Royaume-Uni. Cela est également confirmé par les notes explicatives accompagnant la loi de 2024 sur les pouvoirs d'enquête (modification), dans lesquelles il est précisé que cette modification n'est pas destinée à faire entrer des entreprises supplémentaires dans le champ d'application des compétences pertinentes au titre de l'IPA 2016 ([145]), mais qu'elle est essentiellement fournie à des fins de clarification.

(89) Enfin, la loi de 2024 sur les pouvoirs d'enquête (modification) a apporté certaines modifications ciblées à la procédure de délivrance des mandats, notamment en ce qui concerne l'interception ciblée et le piratage ciblé d'équipements, c'est-à-dire des pouvoirs qui peuvent également être utilisés par des autorités répressives spécifiques au Royaume-Uni aux fins de la prévention ou de la détection des infractions graves. Ces modifications ne concernent que la situation spécifique dans laquelle ces pouvoirs sont utilisés pour obtenir des communications ou des informations privées sur une personne qui est membre d'un organe législatif pertinent ([146]). Bien que les mandats relatifs à l'interception ciblée et au piratage ciblé d'équipements puissent normalement être délivrés par le secrétaire d'État et soient approuvés par un commissaire judiciaire [voir considérants 186 à 196 ainsi que 210 à 215 de la décision d'exécution (UE) 2021/1772], les articles 26 et 111 de l'IPA nécessitent en outre l'approbation du Premier ministre lorsque le mandat concerne un membre du Parlement ou d'un autre organe législatif pertinent (procédure dite «de triple verrouillage»). La loi de 2024 sur les pouvoirs d'enquête (modification) permet désormais au Premier ministre de nommer cinq secrétaires d'État qui seront habilités à exercer le pouvoir du Premier ministre en matière d'autorisation de ces mandats, à condition que la nécessité d'une autorisation soit urgente et que le Premier ministre ne soit pas en mesure de donner son autorisation en raison d'une incapacité médicale ou de l'impossibilité d'accéder à des communications sécurisées. Il est important de noter que les limitations et les garanties relatives à la délivrance de ces mandats qui sont décrites dans les considérants susmentionnés de la décision d'exécution (UE) 2021/1772 restent en vigueur.

3.2.2. *Utilisation ultérieure des informations recueillies*

(90) Le partage de données par une autorité répressive avec une autorité différente à des fins autres que celles pour lesquelles ces données ont été initialement collectées (appelé «partage ultérieur») reste soumis aux conditions analysées aux considérants 142 à 156 de la décision d'exécution (UE) 2021/1772.

([142]) La délivrance de ces avis de conservation au titre des articles 87 à 89 de l'IPA 2016 vise à garantir que les opérateurs de télécommunications conservent, pour une durée maximale de 12 mois, les données de communication pertinentes qui seraient sinon supprimées dès qu'elles ne sont plus nécessaires à des fins commerciales. Les données conservées doivent rester disponibles pendant la durée requise au cas où une autorité publique aurait par la suite besoin de les acquérir au titre d'une autorisation d'acquisition ciblée de données de communication prévue par la partie 3 de l'IPA 2016.

([143]) Article 94A de l'IPA 2016, tel qu'inséré par l'article 20, point 4, de la loi de 2024 sur les pouvoirs d'enquête (modification).

([144]) Article 261, paragraphe 10, point c), de l'IPA 2016, tel que modifié par l'article 19 de la loi de 2024 sur les pouvoirs d'enquête (modification).

([145]) Notes explicatives accompagnant la loi de 2024 sur les pouvoirs d'enquête (modification), point 359, disponibles à l'adresse suivante: https://www.legislation.gov.uk/ukpga/2024/9/pdfs/ukpgaen_20240009_en.pdf.

([146]) Voir articles 26 et 111 de l'IPA 2016.

(91) En ce qui concerne la situation spécifique des transferts ultérieurs du Royaume-Uni vers les États-Unis, 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 (ci-après l'«accord Royaume-Uni/États-Unis») ([147]), conclu en octobre 2019, est entré en vigueur et est mis en œuvre depuis octobre 2022. En vertu de l'accord Royaume-Uni/États-Unis, les données transférées depuis l'Union à des prestataires de services au Royaume-Uni pourraient faire l'objet d'injonctions de production de preuves émises par des autorités répressives américaines et rendues applicables au Royaume-Uni.

(92) Il est important de noter que les conditions et les garanties en vertu desquelles de telles injonctions peuvent être émises et exécutées, qui ont été évaluées au considérant 154 de la décision d'exécution (UE) 2021/1772, continuent de s'appliquer. En particulier, les données obtenues en vertu de l'accord bénéficient de protections équivalentes aux garanties spécifiques prévues par l'accord-cadre UE - États-Unis ([148]), qui sont toutes intégrées dans l'accord Royaume-Uni/États-Unis au moyen d'une référence mutatis mutandis ([149]).

(93) Depuis l'adoption de la décision d'exécution (UE) 2021/1772, le Royaume-Uni a expliqué qu'il avait précisé, grâce notamment aux relations qu'il entretient avec les parties prenantes dans le contexte de la mise en œuvre de l'accord Royaume-Uni/États-Unis, comment les garanties spécifiques prévues par l'accord-cadre, qui ont été conçues pour un contexte de coopération entre les services répressifs, étaient adaptées et appliquées aux transferts spécifiques couverts par l'accord Royaume-Uni/États-Unis. Il a indiqué en particulier que les dispositions de l'accord-cadre qui prévoient un rôle pour l'autorité compétente concernée (qui n'existe pas dans une situation de coopération directe entre un prestataire de services britannique et une autorité répressive aux États-Unis) sont interprétées mutatis mutandis comme faisant référence à l'autorité désignée (telle que définie dans l'accord Royaume-Uni/États-Unis) ([150]) de la partie concernée.

(94) Par exemple, en ce qui concerne la notification d'un incident relatif à la sécurité des informations au titre de l'article 10 de l'accord-cadre UE-États-Unis, qui exige une notification à l'autorité compétente émettrice, le Royaume-Uni a expliqué que cette disposition s'applique mutatis mutandis, de sorte que la notification doit être adressée à l'autorité désignée de la partie ayant transféré les données.

(95) En ce qui concerne l'autorisation de l'autorité compétente émettrice avant tout transfert ultérieur d'informations à caractère personnel conformément à l'article 7 de l'accord-cadre, le Royaume-Uni a précisé qu'il appliquera cette disposition mutatis mutandis afin que l'autorité désignée de la partie ayant transféré les données doive autoriser tout transfert ultérieur.

(96) Pour ce qui est des obligations prévues à l'article 8 de l'accord-cadre concernant la préservation de la qualité et de l'intégrité des informations, il résulterait d'une interprétation mutatis mutandis de cette disposition que l'autorité désignée de la partie qui reçoit les données doit contacter le fournisseur ayant transféré les données en cas de problèmes concernant la qualité et l'intégrité des données.

([147]) 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, disponible à l'adresse suivante: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf.

([148]) 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, ELI: http://data.europa.eu/eli/agree_internation/2016/2220/oj).

([149]) Article 9, paragraphe 1, de l'accord.

([150]) En vertu de l'article 1er, point 8), de l'accord Royaume-Uni/États-Unis, on entend par «autorité désignée» l'entité publique désignée, pour le Royaume-Uni, par le secrétaire d'État à l'Intérieur et, pour les États-Unis, par le procureur général (Attorney General).

(97) En ce qui concerne le recours juridictionnel, le Royaume-Uni a souligné que l'autorité désignée de chaque partie interviendra toujours dans les transferts au titre de l'accord Royaume-Uni/États-Unis. Lorsque les États-Unis sont la partie qui reçoit des données de fournisseurs de services britanniques, le ministère américain de la justice agira en tant qu'autorité désignée. Par conséquent, selon l'interprétation du Royaume-Uni, le ministère de la justice, en tant qu'autorité fédérale désignée en vertu de la loi américaine sur les recours judiciaires, interviendra dans chaque demande émise sur la base de l'accord Royaume-Uni/États-Unis et un recours juridictionnel peut donc être exercé contre le ministère de la justice conformément à l'article 19 de l'accord-cadre. En outre, le Royaume-Uni a confirmé aux services de la Commission que la loi sur les recours judiciaires n'est pas le seul mécanisme de recours. En fonction des circonstances et du contexte de chaque situation, d'autres lois américaines applicables prévoient d'autres voies de recours juridictionnel.

3.2.3. *Surveillance et voies de recours*

(98) En fonction des pouvoirs utilisés par les autorités compétentes lorsqu'elles traitent des données à caractère personnel à des fins répressives (que ce soit au titre de la DPA 2018 ou de l'IPA 2016), différents organes continuent d'assurer la surveillance de l'utilisation de ces pouvoirs, comme indiqué aux considérants 158 à 174 de la décision d'exécution (UE) 2021/1772, et des mécanismes de recours sont toujours prévus par la partie 3 de la DPA 2018 et par l'IPA 2016, ainsi que par la loi de 1998 sur les droits de l'homme, comme indiqué aux considérants 250 à 269 de la décision d'exécution (UE) 2021/1772.

(99) En ce qui concerne la surveillance de la partie 3 de la DPA 2018, les fonctions et les pouvoirs de la commission de l'information sont analysés aux considérants 158 à 160 et 162 de la décision d'exécution (UE) 2021/1772, sous réserve des modifications apportées par la loi sur les données (utilisation et accès) qui sont décrites aux sections 2.3.1 et 2.3.2 de la présente décision.

(100) En ce qui concerne la mise en œuvre de ces pouvoirs, depuis l'adoption de la décision d'exécution (UE) 2021/1772, le commissaire à l'information a traité de nombreuses réclamations ([151]), mené plusieurs enquêtes et pris des mesures d'exécution ayant trait au traitement des données par les autorités répressives. Entre 2021 et 2025, il a diligenté des enquêtes et émis des rappels à l'ordre à l'encontre de divers organes de police pour différents manquements à leurs obligations en matière de protection des données, constatés par exemple lors de la réponse à des demandes d'accès aux données, lors de la mise en place de mesures de sécurité pour les données de vidéosurveillance, lors du traitement de dossiers judiciaires sensibles, lors de la fusion des données de différentes personnes ou lors de la divulgation de données à caractère personnel à des tiers ([152]). Le commissaire à l'information a également publié des lignes directrices, des avis et des documents d'orientation, par exemple sur le droit d'accès ou sur la manière de traiter les demandes manifestement infondées ou excessives au titre de la partie 3 de la DPA 2018 ([153]).

(101) En ce qui concerne l'utilisation des pouvoirs d'enquête au titre de l'IPA 2016, la surveillance indépendante et judiciaire continue d'être assurée par le commissaire aux pouvoirs d'enquête (IPC), qui est assisté par d'autres commissaires judiciaires, désignés collectivement sous le nom de commissaires judiciaires ([154]). Dans ce domaine, la loi de 2024 sur les pouvoirs d'enquête (modification) n'a apporté que des modifications limitées et ciblées, qui ne portent pas atteinte à l'indépendance, aux missions et aux pouvoirs des commissaires judiciaires, mais qui visent à renforcer le fonctionnement dans la pratique du régime de surveillance existant, 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. Ces IPC adjoints doivent être des commissaires judiciaires et sont nommés par l'IPC ([155]).

([151]) Par exemple, en 2023 et 2024, la commission de l'information a reçu 1 890 réclamations sur la base du RGPD et/ou de la DPA 2018 concernant des organisations des sous-secteurs «Autorité de police», «Forces de police» et «Commissaires de police». Voir, également, rapport annuel et états financiers du commissaire à l'information pour la période 2023-2024, disponibles à l'adresse suivante: https://ico.org.uk/media2/migrated/4030348/annual-report-2023-24.pdf.

([152]) De plus amples informations sont disponibles à l'adresse suivante: https://ico.org.uk/action-weve-taken/enforcement/?ensector=criminal-justice.

([153]) Disponibles aux adresses suivantes: https://ico.org.uk/for-organisations/law-enforcement/the-right-of-access-part-3-of-the-dpa-2018/ et https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/individual-rights/manifestly-unfounded-and-excessive-requests/.

([154]) Voir considérant 250 de la décision d'exécution (UE) 2021/1772.

([155]) Article 227 de l'IPA 2016, tel qu'inséré par l'article 7 de la loi sur les pouvoirs d'enquête (modification).

3.3. Évolutions pertinentes concernant l'accès aux données et l'utilisation de celles-ci par les autorités publiques du Royaume-Uni à des fins de sécurité nationale

(102) En ce qui concerne les pouvoirs d'enquête exercés dans le cadre de la sécurité nationale, l'PA 2016 continue de définir le cadre juridique relatif à l'utilisation de ces pouvoirs. Outre les modifications relatives aux pouvoirs d'enquête ciblés qui peuvent également, sous certaines conditions, être utilisés par certaines autorités répressives, comme expliqué aux considérants 77 à 85 de la présente décision, la loi de 2024 sur les pouvoirs d'enquête (modification) a également apporté des modifications à l'un des pouvoirs de masse conférés par l'IPA 2016.

(103) Plus précisément, la loi de 2024 sur les pouvoirs d'enquête (modification) a intégré dans la nouvelle partie 7A de l'IPA 2016 un régime particulier pour la conservation et l'examen d'un sous-ensemble spécifique d'ensembles de données à caractère personnel en masse ([156]), soit des ensembles de données pour lesquels les personnes concernées par les données à caractère personnel ne peuvent raisonnablement pas s'attendre — si ce n'est dans une faible mesure uniquement — à ce que ces données soient privées ([157]). Pour déterminer si un ensemble de données à caractère personnel en masse fait ou non partie d'un tel sous-ensemble spécifique d'ensembles de données, le chef du service de renseignement procède à un examen au regard de toutes les circonstances, en particulier i) la nature des données, ii) la mesure dans laquelle les données ont été rendues publiques par les personnes concernées ou la mesure dans laquelle ces dernières ont consenti à ce que les données soient rendues publiques, iii) la mesure dans laquelle les données, si elles ont été publiées, ont fait l'objet d'un contrôle éditorial ou d'un contrôle de la part d'une personne agissant conformément à des normes professionnelles, iv) la mesure dans laquelle les données, si elles ont été publiées ou relèvent d'une autre manière du domaine public, sont largement connues, et v) la mesure dans laquelle les données ont déjà été utilisées dans le domaine public ([158]).

(104) Il convient de noter que, pour la conservation et l'examen des ensembles de données à caractère personnel en masse ne relevant pas de cette catégorie, c'est-à-dire les données qui sont plus sensibles et dont on peut par conséquent raisonnablement s'attendre à ce qu'elles revêtent un caractère privé, le régime évalué aux considérants 239 et 240 de la décision d'exécution (UE) 2021/1772 reste en place, en particulier la nécessité d'obtenir 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, conformément à la partie 7 de l'IPA 2016 ([159]).

(105) La partie 7A de l'IPA 2016 prévoit deux types d'autorisation, à savoir une autorisation individuelle et une autorisation par catégorie. La conservation, ou la conservation et l'examen, de chaque ensemble de données à caractère personnel en masse détenues en vertu de la partie 7A doivent être autorisés en vertu de l'une de ces autorisations. Les deux autorisations nécessitent en principe ([160]) une autorisation du chef du service de renseignement (ou d'une personne agissant en son nom) et l'approbation d'un commissaire judiciaire indépendant ([161]). Une autorisation individuelle est accordée par le chef d'un service de renseignement sous réserve du respect des conditions énoncées à l'article 226B, paragraphe 4, de l'IPA 2016 et de l'approbation préalable des commissaires judiciaires. Le commissaire judiciaire doit examiner les conclusions de la personne qui a accordé l'autorisation en ce qui concerne la question de savoir si l'article 226A, c'est-à-dire l'attente raisonnable limitée, ou l'absence d'attente raisonnable, quant à l'exigence en matière de respect de la vie privée, s'applique à l'ensemble de données à caractère personnel en masse décrit dans l'autorisation ([162]).

([156]) Les mandats relatifs aux ensembles de données à caractère personnel en masse délivrés conformément à l'article 200 de l'IPA 2016 autorisent les agences de renseignement à conserver et à examiner des ensembles de données qui comprennent des données à caractère personnel concernant un certain nombre de personnes, et la nature de l'ensemble de données est telle que la majorité des personnes ne présentent pas d'intérêt et sont peu susceptibles de présenter un intérêt à l'avenir pour le service de renseignement dans l'exercice de ses fonctions, que l'ensemble de données est conservé électroniquement par un service de renseignement et est détenu à des fins d'analyse dans l'exercice de ses fonctions réglementaires (voir, également, article 199 de l'IPA 2016).

([157]) Article 226A, paragraphe 1, de l'IPA 2016, tel qu'inséré par l'article 2 de la loi de 2024 sur les pouvoirs d'enquête (modification).

([158]) Article 226A, paragraphe 3, de l'a de l'IPA 2016, tel qu'inséré par l'article 2 de la loi de 2024 sur les pouvoirs d'enquête (modification).

([159]) La loi de 2024 sur les pouvoirs d'enquête (modification) a modifié l'article 213 de l'IPA 2016 de manière que les mandats relatifs aux ensembles de données à caractère personnel en masse cessent de produire leurs effets 12 mois après avoir été délivrés. Auparavant, ces mandats devaient être renouvelés tous les 6 mois. Voir l'article 3 de la loi de 2024 sur les pouvoirs d'enquête (modification).

([160]) Une autorisation individuelle peut être accordée sans approbation judiciaire préalable uniquement i) si la personne qui accorde l'autorisation individuelle considère que l'ensemble de données à caractère personnel en masse en question relève d'une autorisation par catégorie existante ou ii) en cas d'urgence [voir la section 226B(6) de l'IPA 2016]. Dans ce dernier cas, la décision d'accorder une autorisation individuelle en urgence doit être examinée par un commissaire judiciaire dans les trois jours ouvrables suivant la date de sa délivrance (voir l'article 226BC de l'IPA 2016).

([161]) Article 226B, paragraphe 1, de l'IPA 2016, tel qu'inséré par l'article 2 de la loi de 2024 sur les pouvoirs d'enquête (modification).

([162]) Article 226BB, paragraphe 1, point a), de l'IPA 2016, tel qu'inséré par l'article 2 de la loi de 2024 sur les pouvoirs d'enquête (modification).

(106) Une autorisation par catégorie autorise la conservation, ou la conservation et l'examen, de la catégorie d'ensembles de données à caractère personnel en masse qu'elle décrit.

(107) La décision d'accorder une telle autorisation par catégorie est prise par le chef du service de renseignement lorsqu'il considère que l'article 226A s'applique à tout ensemble de données relevant de ladite catégorie et que la décision d'accorder l'autorisation est approuvée par un commissaire judiciaire indépendant ([163]). Ce dernier doit examiner si l'article 226A, c'est-à-dire l'attente raisonnable limitée, ou l'absence d'attente raisonnable, quant à l'exigence en matière de respect de la vie privée, s'applique à tout ensemble de données relevant de la catégorie d'ensembles de données décrite dans l'autorisation ([164]).

(108) Il convient de noter que lorsqu'il approuve une décision de délivrance d'une autorisation individuelle ou d'une autorisation par catégorie, le commissaire judiciaire doit «appliquer les mêmes principes que ceux qui seraient appliqués par une juridiction dans le cadre d'une demande de contrôle juridictionnel» ([165]) et examiner ces questions avec un degré de diligence suffisant pour s'assurer de respecter les obligations imposées par l'article 2 de l'IPA 2016 (obligations générales relatives à la protection de la vie privée) ([166]). En outre, la délivrance d'autorisations fait l'objet d'un contrôle ex post strict, au moyen notamment d'un rapport annuel adressé au secrétaire d'État et à la commission du renseignement et de la sécurité du Parlement ([167]), ainsi que d'inspections régulières du Bureau de l'IPC ([168]).

(109) En ce qui concerne les évolutions pertinentes dans le domaine de la surveillance, le Bureau de l'IPC a publié des rapports annuels pour les années 2021, 2022 et 2023, qui fournissent des statistiques et des informations détaillées sur l'utilisation des pouvoirs d'enquête par les agences de renseignement et les services répressifs au Royaume-Uni ([169]). Ces rapports décrivent également les audits et enquêtes menés par le bureau, ainsi que leurs conclusions, et confirment que l'IPC continue d'assurer la fonction très importante de surveillance que lui confère le régime des pouvoirs d'enquête du Royaume-Uni. Par exemple, en 2023, il a contrôlé les justifications invoquées par le quartier général des communications (GCHQ) pour les critères de nécessité et de proportionnalité de l'utilisation des pouvoirs d'interception en masse [tels qu'évalués aux considérants 218 à 225 de la décision d'exécution (UE) 2021/1772] et a conclu qu'une grande majorité des déclarations étaient justifiées par un raisonnement solide, même si, dans certains cas, la proportionnalité n'était pas bien exprimée. Ces conclusions ont été passées en revue avec l'équipe du GCHQ chargée de la conformité, qui s'est engagée à demander une formation de sensibilisation interne supplémentaire afin de remédier à la situation ([170]).

(110) En outre, le tribunal chargé des pouvoirs d'enquête a également publié un rapport public sur ses activités et sa jurisprudence pour la période 2021-2023 ([171]). Il ressort de ce rapport que le nombre d'affaires reçues par le Tribunal a plus que doublé depuis 2017, avec plus de 400 affaires reçues en 2023 ([172]). La plupart des plaintes

([163]) Article 226BA de l'IPA 2016, tel qu'inséré par l'article 2 de la loi de 2024 sur les pouvoirs d'enquête (modification).

([164]) Article 226BB, paragraphe 1, point b), de l'IPA 2016, tel qu'inséré par l'article 2 de la loi de 2024 sur les pouvoirs d'enquête (modification).

([165]) Article 226BB, paragraphe 2, point a), de l'IPA 2016, tel qu'inséré par l'article 2 de la loi de 2024 sur les pouvoirs d'enquête (modification).

([166]) Article 226BB, paragraphe 2, point b), de l'IPA 2016, tel qu'inséré par l'article 2 de la loi de 2024 sur les pouvoirs d'enquête (modification). Conformément aux obligations générales relatives à la protection de la vie privée énoncée à l'article 2 de l'IPA 2016, une autorité publique doit examiner a) si l'objectif visé par le mandat, l'autorisation ou l'avis pourrait être raisonnablement atteint par d'autres moyens moins intrusifs, b) si le niveau de protection requis concernant l'obtention d'informations en vertu du mandat, de l'autorisation ou de l'avis est plus élevé en raison de la nature particulièrement sensible de ces informations en question, c) l'intérêt public en ce qui concerne l'intégrité et la sécurité des systèmes de télécommunication et des services postaux et d) tout autre aspect relevant de l'intérêt public en termes de protection de la vie privée.

([167]) Articles 226DA et 226DB de l'IPA 2016, tel qu'inséré par l'article 2 de la loi de 2024 sur les pouvoirs d'enquête (modification).

([168]) Voir 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, p. 3.

([169]) Les rapports annuels sont disponibles à l'adresse suivante: https://www.ipco.org.uk/publications/annual-reports/.

([170]) Voir points 6.39 à 6.43 du rapport annuel 2023, 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.

([171]) Rapport du tribunal chargé des pouvoirs d'enquête 2021-2023, disponible à l'adresse suivante: https://investigatorypowerstribunal.org.uk/wp-content/uploads/2024/11/Investigatory-Powers-Tribunal-Report-2024.pdf.

([172]) Rapport du tribunal chargé des pouvoirs d'enquête 2021-2023, p. 5.

concernaient des services de répression, suivis de près par les services de sécurité et de renseignement ([173]). Il convient de noter qu'en 2022 et 2023, le Tribunal a rendu des décisions dans des affaires dont il avait été saisi avant 2021, constatant que les autorités publiques du Royaume-Uni [soit, respectivement, la police écossaise ([174]), la police du Grand Manchester ([175]), la police du Surrey ([176]), ainsi que le MI5 et le Home Secretary ([177])] avaient agi illégalement. En ce qui concerne les voies de recours, le tribunal chargé des pouvoirs d'enquête a notamment ordonné la destruction de tout matériel obtenu illégalement et, dans un cas, le paiement de 12 000 GBP à titre de satisfaction équitable pour les violations constatées. Le rapport annuel confirme donc que le tribunal chargé des pouvoirs d'enquête remplit effectivement son rôle important consistant à garantir la surveillance et les voies de recours dans le domaine de l'application du droit pénal et de l'accès aux données à caractère personnel à des fins de sécurité nationale.

(111) En outre, le rapport souligne également d'importants développements, parmi lesquels un arrêt de la Cour européenne des droits de l'homme selon lequel toute personne, où qu'elle soit dans le monde, peut saisir le tribunal chargé des pouvoirs d'enquête concernant la mise en œuvre du régime d'interception en masse du Royaume-Uni si les agissements visés sont le fait d'une instance publique du Royaume-Uni et se sont produits au Royaume-Uni ([178]).

4. **CONCLUSION**

(112) La Commission considère que le RGPD britannique et la DPA 2018, tels que modifiés par la loi sur les données (utilisation et accès), continuent d'assurer un niveau de protection des données à caractère personnel transférées depuis l'Union européenne essentiellement équivalent à celui garanti par le règlement (UE) 2016/679.

(113) De plus, la Commission considère que, pris dans leur ensemble, les mécanismes de surveillance et les voies de recours prévus dans le droit britannique permettent encore d'identifier et de sanctionner en pratique les infractions et offrent toujours aux personnes concernées des voies de droit leur permettant d'avoir accès aux données à caractère personnel les concernant et, in fine, d'obtenir leur rectification ou leur effacement.

(114) Enfin, sur la base des informations disponibles concernant l'ordre juridique du Royaume-Uni, la Commission considère que toute ingérence dans les droits fondamentaux des personnes dont les données à caractère personnel sont transférées depuis l'Union européenne vers le Royaume-Uni par les autorités publiques britanniques pour des motifs d'intérêt public, en particulier à des fins répressives et à des fins de sécurité nationale, continue d'être limitée à ce qui est strictement nécessaire pour atteindre l'objectif légitime en question et qu'une protection juridictionnelle effective existe contre une telle ingérence.

(115) Dès lors, vu les constatations de la présente décision, il convient de décider que le Royaume-Uni continue de garantir un niveau de protection adéquat au sens de l'article 45 du règlement (UE) 2016/679, interprété à la lumière de la Charte des droits fondamentaux de l'Union européenne.

(116) Cette conclusion se fonde à la fois sur le régime national applicable du Royaume-Uni, tel qu'il a évolué depuis l'adoption de la décision d'exécution (UE) 2021/1772, et sur ses engagements internationaux, notamment le maintien de l'adhésion du Royaume-Uni à la convention européenne des droits de l'homme et le maintien de sa soumission à la compétence de la Cour européenne des droits de l'homme. Le respect permanent de ces obligations internationales constitue donc un élément particulièrement important de l'évaluation sur laquelle est fondée la présente décision.

([173]) Rapport du tribunal chargé des pouvoirs d'enquête 2021-2023, p. 12.
([174]) Wilson/Police Scotland [2022] UKIPTrib 5.
([175]) Pendlebury/Greater Manchester Police [2023] UKIPTrib 2.
([176]) Hill/Metropolitan Police Service & Independent Office For Police Conduct [2022] UKIPTrib 6.
([177]) Liberty & Privacy International/Security Service and Secretary of State for the Home Department [2023] UKIPTrib 1.
([178]) Wieder et Guarnieri/Royaume-Uni, [2023] CEDH 668; voir également le rapport du tribunal chargé des pouvoirs d'enquête 2021-2023, p. 6.

5. EFFETS DE LA PRÉSENTE DÉCISION ET ACTION DES AUTORITÉS DE PROTECTION DES DONNÉES

(117) Les États membres et leurs organes sont tenus de prendre les mesures nécessaires pour se conformer aux actes des institutions de l'Union, car ces derniers jouissent d'une présomption de légalité et produisent, dès lors, des effets juridiques aussi longtemps qu'ils n'ont pas expiré, été retirés, été annulés à la suite d'un recours en annulation ou été déclarés invalides à la suite d'un renvoi préjudiciel ou d'une exception d'illégalité.

(118) En conséquence, une décision d'adéquation de la Commission adoptée en vertu de l'article 45, paragraphe 3, du règlement (UE) 2016/679 a un caractère contraignant pour tous les organes des États membres destinataires, y compris leurs autorités de surveillance indépendantes. En particulier, au cours de la période d'application de la décision d'exécution (UE) 2021/1772, modifiée par la présente décision, les transferts d'un responsable du traitement ou d'un sous-traitant situé dans l'Union européenne à des responsables du traitement ou des sous-traitants situés au Royaume-Uni peuvent avoir lieu sans qu'il soit nécessaire d'obtenir une autorisation supplémentaire.

(119) Il convient de rappeler que, comme prévu à l'article 58, paragraphe 5, du règlement (UE) 2016/679 et ainsi que la Cour de justice l'a expliqué dans l'arrêt Schrems I ([179]), lorsqu'une autorité nationale chargée de la protection des données met en cause, notamment après avoir été saisie d'une plainte, la compatibilité d'une décision d'adéquation de la Commission avec la protection des droits fondamentaux que constituent le respect de la vie privée et la protection des données, le droit national doit prévoir des voies de recours lui permettant de faire valoir ces griefs devant les juridictions nationales, qui peuvent être tenues de procéder à un renvoi préjudiciel devant la Cour de justice ([180]).

6. SUIVI

(120) Conformément à l'article 45, paragraphe 4, du règlement (UE) 2016/679, la Commission doit suivre, de manière permanente, les évolutions pertinentes au Royaume-Uni afin de déterminer si ce pays continue d'assurer un niveau de protection essentiellement équivalent. Ce suivi est d'autant plus important que le Royaume-Uni appliquera et mettra en œuvre un régime modifié de protection des données. En outre, le cadre de protection des données modifié du Royaume-Uni confère au secrétaire d'État le pouvoir de préciser davantage le cadre au moyen du droit dérivé. À cet égard, il convient d'accorder une attention particulière à de telles spécifications supplémentaires, ainsi qu'à l'application concrète des règles modifiées du Royaume-Uni concernant les transferts des données à caractère personnel aux pays tiers, à l'exercice effectif des droits individuels, y compris toute évolution pertinente de la législation et de la pratique concernant les exceptions ou restrictions à ces droits nouvellement introduites, au fonctionnement de l'ICO restructuré, y compris en ce qui concerne le traitement des plaintes et l'application des mesures correctives, ainsi que le respect des limites et des garanties en matière d'accès des pouvoirs publics, en particulier pour ce qui est de la partie 7A de l'IPA 2016 introduite récemment. Parmi d'autres éléments, la Commission devrait fonder son suivi sur les évolutions de la jurisprudence et sur la surveillance exercée par l'ICO et par d'autres organismes indépendants.

(121) Pour faciliter ce suivi, les autorités britanniques devraient informer rapidement la Commission de toute modification de fond apportée à l'ordre juridique du Royaume-Uni ayant une incidence sur le cadre juridique qui fait l'objet de la décision d'exécution (UE) 2021/1772, telle que modifiée par la présente décision, ainsi que de toute évolution des pratiques relatives au traitement des données à caractère personnel évaluées dans la décision d'exécution (UE) 2021/1772, telle que modifiée par la présente décision, en ce qui concerne tant le traitement des données à caractère personnel par les responsables du traitement et les sous-traitants au titre du RGPD britannique que les limitations et garanties applicables à l'accès des autorités publiques aux données à caractère personnel. Cela devrait comprendre toute évolution concernant les éléments mentionnés au considérant 120.

(122) En outre, afin de permettre à la Commission d'accomplir efficacement sa mission de suivi, les États membres devraient l'informer de toute mesure pertinente prise par les autorités nationales chargées de la protection des données, en particulier en ce qui concerne les requêtes ou les plaintes des personnes concernées de l'Union ayant trait au transfert de données à caractère personnel de l'Union à des responsables du traitement ou à des sous-traitants au Royaume-Uni. La Commission devrait également être informée de tout élément indiquant que les mesures prises par les autorités publiques du Royaume-Uni qui sont responsables de la prévention et de la détection des infractions pénales, ainsi que des enquêtes et des poursuites en la matière, y compris les organes de supervision, n'assurent pas le niveau de protection requis.

([179]) Arrêt Schrems I, point 65.

([180]) Arrêt Schrems I, point 65: «À cet égard, il incombe au législateur national de prévoir des voies de recours permettant à l'autorité nationale de contrôle concernée de faire valoir les griefs qu'elle estime fondés devant les juridictions nationales afin que ces dernières procèdent, si elles partagent les doutes de cette autorité quant à la validité de la décision de la Commission, à un renvoi préjudiciel aux fins de l'examen de la validité de cette décision.»

(123) Lorsque les informations disponibles, en particulier les informations résultant du suivi de la décision d'exécution (UE) 2021/1772, telle que modifiée par la présente décision, ou fournies par les autorités du Royaume-Uni ou des États membres, révèlent que le niveau de protection assuré par le Royaume-Uni pourrait ne plus être adéquat, la Commission devrait en informer rapidement les autorités compétentes du Royaume-Uni et demander que des mesures appropriées soient prises dans un délai raisonnable bien défini, qui ne devrait pas excéder trois mois. Ce délai peut au besoin être prorogé pour une durée déterminée, compte tenu de la nature de la question en cause et/ou des mesures à prendre. Ainsi, une telle procédure pourrait être déclenchée dans la mesure où des transferts ultérieurs, y compris des transferts effectués sur la base de nouveaux règlements d'adéquation adoptés par le secrétaire d'État ou des accords internationaux conclus par le Royaume-Uni, ne s'accompagneraient plus de garanties quant à la continuité de la protection au sens de l'article 44 du règlement (UE) 2016/679.

(124) Si, à l'expiration de la période précisée, les autorités britanniques compétentes n'ont pas pris ces mesures ou échouent à démontrer de manière satisfaisante que la présente décision reste fondée sur un niveau de protection adéquat, la Commission lancera la procédure visée à l'article 93, paragraphe 2, du règlement (UE) 2016/679 en vue de la suspension partielle ou complète ou de l'abrogation de la présente décision.

(125) À défaut, la Commission lancera cette procédure en vue de modifier la présente décision, notamment en soumettant les transferts de données à des conditions supplémentaires ou en limitant le constat d'adéquation aux seuls transferts de données pour lesquels un niveau de protection adéquat continue d'être assuré.

(126) Pour des raisons d'urgence impérieuse dûment justifiées, la Commission aura recours à la possibilité d'adopter, conformément à la procédure visée à l'article 93, paragraphe 3, du règlement (UE) 2016/679, des actes d'exécution immédiatement applicables suspendant, abrogeant ou modifiant la décision.

7. **RÉEXAMEN, DURÉE ET RENOUVELLEMENT DE LA PRÉSENTE DÉCISION**

(127) En application de l'article 45, paragraphe 3, du règlement (UE) 2016/679, et au regard du fait que le niveau de protection assuré par le cadre juridique du Royaume-Uni est susceptible d'évoluer, la Commission, après l'adoption de la présente décision, devrait vérifier de manière périodique si les conclusions relatives au niveau adéquat de la protection assurée par le Royaume-Uni sont toujours justifiées en fait et en droit, compte tenu des éléments énumérés à l'article 45, paragraphe 2, du règlement (UE) 2016/679. Ces évaluations devraient avoir lieu au moins une fois tous les quatre ans et couvrir tous les aspects relatifs au fonctionnement de la présente décision, y compris le fonctionnement des mécanismes de surveillance et d'application pertinents.

(128) Aux fins de cet examen, la Commission devrait rencontrer les représentants permanents des autorités du Royaume-Uni, y compris la commission de l'information. La participation à cette réunion devrait être ouverte aux représentants des membres du comité européen de la protection des données. Dans le cadre de l'examen, la Commission devrait demander au Royaume-Uni de fournir des informations exhaustives sur tous les aspects pertinents pour le constat d'adéquation. La Commission devrait également demander des explications sur toute information reçue présentant de l'intérêt pour la présente décision, notamment de la part de l'EDPB, de diverses autorités de protection des données ou de groupes de la société civile, des informations publiques ou relayés par les médias, ou toute autre source d'informations disponible.

(129) Sur la base de l'examen, la Commission devrait élaborer un rapport public qui sera présenté au Parlement européen et au Conseil.

(130) La Commission doit également tenir compte du fait que le cadre de protection des données évalué dans la présente décision et dans la décision d'exécution (UE) 2021/1772 peut encore évoluer.

(131) Il convient donc de disposer que la présente décision est applicable pour une durée de six ans à compter de son entrée en vigueur.

(132) Plus particulièrement, si les informations issues du suivi de la présente décision révèlent que les constatations relatives à l'adéquation du niveau de protection assuré au Royaume-Uni sont toujours justifiées sur les plans factuel et juridique, la Commission devrait, au moins six mois avant l'expiration de la présente décision, lancer la procédure de modification de la présente décision en prorogeant sa portée dans le temps, en principe, d'une durée supplémentaire de quatre ans. Un tel acte d'exécution modifiant ainsi la présente décision doit être adopté conformément à la procédure visée à l'article 93, paragraphe 2, du règlement (UE) 2016/679.

8. **CONSIDÉRATIONS FINALES**

(133) Le comité européen de la protection des données a publié un avis ([181]), dont il a été tenu compte dans l'élaboration de la présente décision.

(134) La mesure prévue par la présente décision est conforme à l'avis du comité institué par l'article 93 du règlement (UE) 2016/679.

(135) Il y a donc lieu de modifier la décision d'exécution (UE) 2021/1772 en conséquence,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

L'article 1er, paragraphe 2, de la décision d'exécution (UE) 2021/1772 est abrogé.

Article 2

L'article 4 de la décision d'exécution (UE) 2021/1772 est remplacé par le texte suivant:

«*Article 4*

La présente décision expire le 27 décembre 2031, sauf si elle est prorogée conformément à la procédure visée à l'article 93, paragraphe 2, du règlement (UE) 2016/679.».

Article 3

Les États membres sont destinataires de la présente décision.

Fait à Bruxelles, le 19 décembre 2025.

Par la Commission
Michael MCGRATH
Membre de la Commission

([181]) Avis 26/2025 concernant le projet de décision d'exécution de la Commission européenne modifiant le règlement (UE) 2016/679, le niveau de protection adéquat des données à caractère personnel assuré par le Royaume-Uni, disponible à l'adresse suivante: https://www.edpb.europa.eu/system/files/2025-10/edpb_opinion_202526_united_kingdom_adequacy_gdpr_en.pdf.