COMMISSION
EUROPÉENNE

Bruxelles, le 28.6.2021
C(2021) 4800 final

DÉCISION D'EXÉCUTION DE LA COMMISSION

du 28.6.2021

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

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

DÉCISION D'EXÉCUTION DE LA COMMISSION

du 28.6.2021

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

(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) (RGPD)[1], et notamment son article 45, paragraphe 3,

considérant ce qui suit:

1. INTRODUCTION

(1) Le règlement (UE) 2016/679 fixe les règles applicables au transfert de données à caractère personnel, par des responsables du traitement ou des sous-traitants au sein de l'Union européenne, vers des pays tiers et à des organisations internationales, dans la mesure où ces transferts relèvent de son champ d'application. Les règles relatives aux transferts internationaux de données sont définies au chapitre V dudit règlement, soit aux articles 44 à 50. Bien que les flux de données à caractère personnel en provenance et à destination de pays non-membres de l'Union européenne soient nécessaires au développement de la coopération internationale et des échanges commerciaux transfrontières, le niveau de protection assuré aux données à caractère personnel au sein de l'Union européenne ne doit pas être compromis par des transferts vers des pays tiers[2].

(2) En vertu de l'article 45, paragraphe 3, du règlement (UE) 2016/679, la Commission peut décider, par voie d'actes d'exécution, qu'un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans un pays tiers, ou une organisation internationale, assure un niveau de protection adéquat. Dans cette circonstance, les transferts de données à caractère personnel vers un pays tiers peuvent avoir lieu sans qu'il soit nécessaire d'obtenir une autre autorisation, comme prévu à l'article 45, paragraphe 1, et au considérant 103 dudit règlement.

(3) Comme précisé à l'article 45, paragraphe 2, du règlement (UE) 2016/679, l'adoption d'une décision d'adéquation doit reposer sur une analyse approfondie de l'ordre juridique du pays tiers, en ce qui concerne tant les règles applicables aux importateurs de données que les limitations et les garanties en matière d'accès des autorités

[1] JO L 119 du 4.5.2016, p. 1.

[2] Voir le considérant 101 du règlement (UE) 2016/679.

publiques aux données à caractère personnel. Dans son évaluation, 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 [considérant 104 du règlement (UE) 2016/679]. La norme au regard de laquelle l'«équivalence essentielle» est évaluée est celle fixée par la législation de l'Union européenne, notamment le règlement (UE) 2016/679, ainsi que la jurisprudence de la Cour de justice de l'Union européenne (CJUE)[3]. Les critères de référence pour l'adéquation du comité européen de la protection des données sont également importants à cet égard[4].

(4) Comme l'a précisé la Cour de justice de l'Union européenne, il n'est pas nécessaire de constater un niveau de protection identique[5]. 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[6]. 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 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[7].

(5) La Commission a soigneusement analysé la législation et les pratiques du Royaume-Uni. Sur la base des constatations exposées aux considérants (8) à (270), la Commission conclut que le Royaume-Uni assure un niveau de protection adéquat des données à caractère personnel transférées dans le cadre du champ d'application du règlement (UE) 2016/679 de l'Union européenne vers le Royaume-Uni.

(6) Cette conclusion ne concerne 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 (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. La validité et l'interprétation de l'exemption en matière d'immigration en droit britannique ne sont pas tranchées à la suite d'une décision de la Cour d'appel d'Angleterre et du pays de Galles du 26 mai 2021. Tout en reconnaissant que les droits des personnes concernées peuvent, en principe, être limités aux fins du contrôle de l'immigration en tant qu'«aspect important de l'intérêt public», la Cour d'appel a jugé que l'exemption en matière d'immigration est, dans sa forme actuelle, incompatible avec le droit britannique, étant donné que la mesure législative ne contient pas de dispositions spécifiques énonçant

---

3 Voir plus récemment l'arrêt de la Cour dans l'affaire C-311/18, Facebook Ireland et Schrems (ci-après l'«arrêt Schrems II»), ECLI:EU:C:2020:559.

4 Comité européen de la protection des données, Critères de référence pour l'adéquation, WP 254 rev. 01, disponibles à l'adresse suivante: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

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

6 Arrêt Schrems I, point 74.

7 Voir la communication de la Commission au Parlement européen et au Conseil, 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/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN.

les garanties énumérées à l'article 23, paragraphe 2, du règlement général sur la protection des données du Royaume-Uni (RGPD britannique)[8]. Dans ces conditions, les transferts de données à caractère personnel de l'Union vers le Royaume-Uni auxquels l'exemption en matière d'immigration peut s'appliquer devraient être exclus du champ d'application de la présente décision[9]. Une fois qu'il aura été remédié à l'incompatibilité avec le droit britannique, l'exemption en matière d'immigration devrait être réexaminée, de même que la nécessité de maintenir la limitation du champ d'application de la présente décision.

(7) La présente décision ne devrait avoir aucune incidence sur l'application directe du règlement (UE) 2016/679 aux organisations établies au Royaume-Uni lorsque les conditions relatives au champ d'application territorial dudit règlement, défini à son article 3, sont remplies.

2. RÈGLES APPLICABLES AU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

2.1. Le cadre constitutionnel

(8) Le Royaume-Uni est une démocratie parlementaire dont le chef d'État est un souverain constitutionnel. Le Royaume-Uni possède un Parlement souverain, qui exerce une autorité suprême sur l'ensemble des autres institutions gouvernementales, un pouvoir exécutif issu et sous l'autorité du Parlement, ainsi qu'un pouvoir judiciaire indépendant. Le pouvoir exécutif tire son autorité de sa capacité à obtenir la confiance de la Chambre des communes élue. Il rend compte aux deux chambres du Parlement qui sont chargées de contrôler l'action du gouvernement, ainsi que d'examiner et de voter les lois.

(9) Le Parlement britannique a transféré des responsabilités au Parlement écossais, au Parlement gallois (Senedd Cymru) et à l'Assemblée d'Irlande du Nord afin que ceux-ci puissent légiférer en Écosse, au Pays de Galles et en Irlande du Nord sur des points concernant les affaires intérieures qu'il ne s'est pas réservés. Bien que la protection des données soit un point réservé, c'est-à-dire que la même législation s'applique dans tout le pays, d'autres domaines politiques en rapport avec la présente décision sont décentralisés. Par exemple, les systèmes de justice pénale, y compris les fonctions de police, de l'Écosse et de l'Irlande du Nord sont délégués respectivement au Parlement écossais et à l'Assemblée d'Irlande du Nord. Le Royaume-Uni ne possède pas de constitution codifiée à proprement parler. Les principes constitutionnels, apparus au fil du temps, sont tirés de la jurisprudence et des conventions en particulier. La valeur constitutionnelle de certaines lois, telles que la Magna Carta (Grande Charte), la Déclaration des droits de 1689 et la loi de 1998 sur les droits de l'homme, a été reconnue par les tribunaux. Les droits fondamentaux des personnes ont été établis, en tant que partie intégrante de la constitution, par la *common law*, lesdites lois et les

---

[8] Court of Appeal (Civil Division), *Open Rights Group v Secretary of State for the Home Department and Secretary of State for Digital, Culture, Media and Sport,* [2021] EWCA Civ 800, points 53 à 56. La Cour d'appel a infirmé la décision de la Haute Cour de justice qui avait précédemment apprécié l'exemption à la lumière du règlement (UE) 2016/679 (en particulier de son article 23) et de la Charte des droits fondamentaux de l'Union européenne et avait conclu à la légalité de l'exemption (*Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor* [2019] EWHC 2562).

[9] Pour autant que les conditions applicables soient remplies, les transferts à des fins de contrôle de l'immigration au Royaume-Uni peuvent être effectués sur la base des mécanismes de transfert prévus aux articles 46 à 49 du règlement (UE) 2016/679.

traités internationaux, notamment la convention européenne des droits de l'homme (CEDH) que le Royaume-Uni a ratifiée en 1951. Le Royaume-Uni a également ratifié la convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (convention 108) en 1987[10].

(10) 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 (ainsi que le droit à la protection des données qui fait partie dudit droit) et le droit à un procès équitable[11]. En particulier, conformément à l'article 8 de ladite convention, il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence soit prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.

(11) Conformément à la loi de 1998 sur les droits de l'homme, toute action des autorités publiques doit être compatible avec un droit garanti par la convention[12]. En outre, la législation primaire et la législation dérivée doivent être interprétées et appliquées de manière compatible avec les droits reconnus par la convention[13].

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

(12) Le Royaume-Uni s'est retiré de l'Union européenne le 31 janvier 2020. En vertu de l'accord de 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[14], le droit de l'Union demeure applicable au Royaume-Uni pendant la période de transition jusqu'au 31 décembre 2020. Avant le retrait et pendant la période de transition, le cadre législatif en matière de protection des données à caractère personnel au Royaume-Uni se composait de la législation de l'Union en vigueur [en particulier, le règlement (UE) 2016/679 et la directive (UE) 2016/680 du Parlement européen et du

---

10 Les principes de la convention 108 ont été initialement transposés dans le droit britannique par la loi de 1984 sur la protection des données, laquelle a été remplacée par la loi de 1998 sur la protection des données (DPA 1998), puis par la loi de 2018 sur la protection des données (DPA 2018) (lue en combinaison avec le RGPD britannique). Le Royaume-Uni a par ailleurs signé, en 2018, le protocole d'amendement à la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (appelé convention 108+) et œuvre actuellement à la ratification de la convention.

11 Articles 6 et 8 de la CEDH (voir également l'annexe 1 de la loi de 1998 sur les droits de l'homme).

12 Article 6 de la loi de 1998 sur les droits de l'homme.

13 Article 3 de la loi de 1998 sur les droits de l'homme.

14 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 (2019/C 384 I/01), XT/21054/2019/INIT (JO C 384I du 12.11.2019, p. 1), disponible à l'adresse suivante: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=EN

Conseil[15]] et de la législation nationale, notamment la loi de 2018 sur la protection des données (DPA 2018)[16] qui 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.

(13) Afin de préparer le retrait de l'Union européenne, le gouvernement britannique a promulgué la loi de 2018 sur l'Union européenne (notification de retrait)[17], qui intègre la législation de l'Union directement applicable dans le droit britannique[18]. Ce «droit de l'Union conservé» inclut l'intégralité du règlement (UE) 2016/679 (y compris ses considérants)[19]. Conformément à cette loi, le droit de l'Union qui aura été conservé sans modifications doit 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 sont 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»)[20].

(14) En vertu de la loi de 2018 sur l'Union européenne (notification de retrait), les ministres du Royaume-Uni ont le pouvoir d'adopter des législations secondaires, par voie d'actes réglementaires, afin d'apporter les modifications nécessaires au droit de l'Union européenne conservé à la suite du retrait du Royaume-Uni de l'Union européenne. Ils ont exercé ce pouvoir en adoptant la réglementation de 2019 sur la protection des données, la vie privée et les communications électroniques (modifications, etc.) (sortie de l'Union) (réglementation DPPEC)[21]. Cette

---

15 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, p. 89), disponible à l'adresse suivante: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN .

16 Loi de 2018 sur la protection des données, disponible à l'adresse suivante: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

17 Loi de 2018 sur le retrait de l'Union européenne, disponible à l'adresse suivante: https://www.legislation.gov.uk/ukpga/2018/16/contents.

18 La loi de 2018 sur l'Union européenne (notification de retrait) a pour but et pour effet d'intégrer dans le droit britannique toute la législation directe de l'Union qui était intégrée dans le droit britannique à la fin de la période de transition étant donné qu'elle est d'effet immédiat en droit de l'Union avant la fin de la période de transition [voir l'article 3 de la loi de 2018 sur l'Union européenne (retrait)].

19 Les notes explicatives de la loi de 2018 sur l'Union européenne (notification de retrait) précisent que: «Lorsqu'une législation est transposée en vertu de cet article, c'est le texte de la législation lui-même qui fera partie de la législation nationale. Cela inclura le texte intégral de tout instrument de l'Union (y compris ses considérants)». [Notes explicatives de 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]. Selon les informations communiquées par les autorités britanniques, étant donné que les considérants n'ont pas le statut de règles juridiques contraignantes, il n'était pas nécessaire de les modifier de la même façon que les articles du règlement (UE) 2016/679 ont été modifiés par la réglementation de 2019 sur la protection des données, la vie privée et les communications électroniques (DPPEC).

20 Article 6 de la loi de 2018 sur l'Union européenne (notification de retrait).

21 Réglementation de 2019 sur la protection des données, la vie privée et les communications électroniques (modifications, etc.) (sortie de l'Union), disponible à l'adresse suivante: https://www.legislation.gov.uk/uksi/2019/419/contents/made, telle que modifiée par la réglementation DPPEC 2020, disponible à l'adresse suivante: https://www.legislation.gov.uk/ukdsi/2020/9780348213522.

réglementation 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[22].

(15) Par conséquent, après la fin de la période de transition, le cadre juridique en matière de protection des données à caractère personnel du Royaume-Uni se compose:

– du RGPD britannique, tel qu'il a été intégré dans le droit britannique en vertu de la loi de 2018 sur l'Union européenne (notification de retrait) et modifié par la réglementation DPPEC[23], et

– de la DPA 2018[24], telle que modifiée par la réglementation DPPEC.

(16) Étant donné que le RGPD britannique est fondé sur le droit de l'Union, les règles du Royaume-Uni en matière de protection des données sont très semblables, à de nombreux égards, aux règles correspondantes applicables au sein de l'Union européenne.

(17) Outre les pouvoirs conférés au secrétaire d'État par la loi de 2018 sur l'Union européenne (notification de retrait), plusieurs dispositions de la DPA 2018 confèrent à celui-ci le pouvoir d'adopter des législations secondaires en vue de modifier certaines dispositions de ladite loi ou d'introduire des règles complémentaires et additionnelles[25]. Le secrétaire d'État n'a exercé jusqu'ici que le pouvoir visé à l'article 137 de la DPA 2018 consistant à adopter la réglementation de 2019 sur la protection des données (redevances et informations) (modification), qui précise les circonstances dans lesquelles les responsables du traitement sont tenus de verser une redevance annuelle à l'autorité indépendante britannique de protection des données, le commissaire à l'information.

(18) Enfin, les codes de bonnes pratiques et autres orientations adoptés par le commissaire à l'information contiennent des orientations supplémentaires relatives à la législation du Royaume-Uni en matière de protection des données. Bien qu'elles ne soient pas formellement contraignantes sur le plan juridique, ces orientations influent sur l'interprétation de la législation en matière de protection des données et décrivent la

---

22 Ces modifications du RGPD britannique et de la DPA 2018, qui sont essentiellement de nature technique, consistent notamment à supprimer les références aux «États membres» ou à adapter la terminologie, en remplaçant par exemple les références au règlement (UE) 2016/679 par des références au RGPD britannique. Dans certains cas, des changements étaient nécessaires afin de refléter le contexte purement national des dispositions, par exemple en ce qui concerne la personne «qui» adopte les «règlements d'adéquation» aux fins du cadre législatif britannique en matière de protection des données (voir l'article 17A de la DPA 2018), à savoir le ministre en lieu et place de la Commission européenne.

23 Règlement général sur la protection des données, version modifiée (Keeling Schedule), disponible à l'adresse suivante: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946117/20201102_-_GDPR_-_MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf.

24 Loi de 2018 sur la protection des données, version modifiée (Keeling Schedule), disponible à l'adresse suivante: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946100/20201102_-_DPA_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf.

25 Ces pouvoirs sont énoncés, par exemple, aux articles 16 (pouvoir d'appliquer, dans des circonstances particulières, étroitement encadrées, des exemptions supplémentaires à certaines dispositions du RGPD britannique), 17A (pouvoir d'adopter des règlements d'adéquation), 212 et 213 (pouvoirs de fixer la date d'entrée en vigueur et d'appliquer des dispositions transitoires), ainsi que 211 (pouvoir d'apporter des modifications mineures et consécutives) de la DPA 2018.

manière dont elle est appliquée et mise en œuvre, en pratique, par le commissaire. Les articles 121 à 125 de la DPA 2018 obligent notamment le commissaire à préparer des codes de bonnes pratiques relatifs au partage des données, à la prospection, à la conception adaptée aux enfants, ainsi qu'à la protection des données et au journalisme.

(19) Au niveau de sa structure et de ses principaux éléments, le cadre juridique du Royaume-Uni applicable aux données transférées au titre de la présente décision est donc très semblable à celui qui s'applique dans l'Union européenne. Ainsi, ce cadre est non seulement fondé sur des obligations prévues dans le droit interne, qui ont été façonnées par le droit de l'Union, mais également sur des obligations consacrées par le droit international, notamment dans le cadre de l'adhésion du Royaume-Uni à la CEDH et à la convention 108, ainsi que de sa soumission à la compétence de la Cour européenne des droits de l'homme. Ces obligations découlant d'instruments internationaux juridiquement contraignants, qui concernent notamment la protection des données à caractère personnel, constituent donc un élément particulièrement important du cadre juridique évalué dans la présente décision.

2.3. Champ d'application matériel et territorial

(20) Tout comme le règlement (UE) 2016/679, le RGPD britannique s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ou à d'autres traitements, si les données à caractère personnel sont contenues dans un fichier[26]. Les définitions de «données à caractère personnel», de «personne concernée» et de «traitement» figurant dans le RGPD britannique sont identiques à celles du règlement (UE) 2016/679[27]. De plus, le RGPD britannique s'applique au traitement manuel non structuré des données à caractère personnel[28] détenues par certaines autorités publiques du Royaume-Uni[29], bien que les droits et principes énoncés dans le RGPD britannique qui ne sont pas pertinents pour de telles données soient écartés par les articles 24 et 25 de la DPA 2018. À l'instar de ce que prévoit le règlement (UE) 2016/679, le RGPD britannique ne s'applique pas aux traitements de données à caractère personnel effectués par une personne physique au cours d'activités strictement personnelles ou domestiques[30].

(21) Le RGPD britannique étend également son champ d'application aux traitements au cours d'activités qui, immédiatement avant la fin de la période de transition, ne relevaient pas du champ d'application du droit de l'Union européenne (par exemple, des activités liées à la sécurité nationale)[31], ou qui relevaient du champ d'application

---

26 Article 2, paragraphes 1 et 5, du RGPD britannique.

27 Article 4, paragraphes 1 et 2, du RGPD britannique.

28 L'article 2, paragraphe 5, point b), définit le traitement manuel non structuré de données à caractère personnel comme le traitement autre que le traitement automatisé ou structuré de données à caractère personnel.

29 Conformément à l'article 2, paragraphe 1A, du RGPD britannique, le règlement s'applique également au traitement manuel non structuré des données à caractère personnel détenues par une autorité publique au sens de la loi sur la liberté de l'information. La référence aux autorités publiques au sens de la loi sur la liberté de l'information désigne toute autorité publique telle qu'elle est définie dans la loi de 2000 sur la liberté de l'information, ou toute autorité publique écossaise telle qu'elle est définie dans la loi écossaise de 2002 sur la liberté de l'information (loi du Parlement écossais 13). Article 21, paragraphe 5, de la DPA 2018.

30 Article 2, paragraphe 2, point a), du RGPD britannique.

31 Les activités liées à la sécurité nationale relèvent uniquement du champ d'application du RGPD britannique, dans la mesure où elles ne sont pas exercées par une autorité

du titre V, chapitre 2, du traité sur l'Union européenne (activités relatives à la politique étrangère et de sécurité commune)[32]. Comme dans le système de l'Union européenne, le RGPD britannique ne s'applique pas au traitement de données à caractère personnel effectué par une autorité compétente 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 des menaces pour la sécurité publique et la prévention de telles menaces (ci-après «à des fins répressives») – ce type de traitement est en revanche régi par la partie 3 de la DPA 2018, de même qu'il est régi par la directive (UE) 2016/680 en vertu du droit de l'Union européenne – ou au traitement de données à caractère personnel par des services de renseignement [le *Security Service* (MI5), le *Secret Intelligence Service* (SIS) et le *Government Communications Headquarters* (GCHQ)] qui est couvert par la partie 4 de la DPA 2018[33].

(22) Le champ d'application territorial du RGPD britannique est décrit à l'article 3 de cet acte[34] et comprend le traitement de données à caractère personnel (quel que soit le lieu du traitement) effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire du Royaume-Uni, ainsi que le traitement de données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire du Royaume-Uni, lorsque les activités de traitement sont liées à l'offre de biens ou de services à ces personnes, ou au suivi du comportement de ces personnes[35]. Cette approche reflète celle adoptée à l'article 3 du règlement (UE) 2016/679.

2.4. Définitions de «données à caractère personnel» et des notions de «responsable du traitement» et de «sous-traitant»

(23) Les définitions de «données à caractère personnel», de «traitement», de «responsable du traitement», de «sous-traitant», ainsi que la définition de «pseudonymisation», énoncées dans le règlement (UE) 2016/679, ont été conservées dans le RGPD britannique sans modifications substantielles[36]. En outre, les catégories particulières de

---

compétente à des fins répressives, auquel cas la partie 3 de la DPA 2018 s'applique, ou par un service de renseignement ou pour le compte de celui-ci, dont les activités sont exclues du champ d'application du RGPD britannique et relèvent de la partie 4 de la DPA 2018, conformément à l'article 2, paragraphe 2, point c), du RGPD britannique. Par exemple, les forces de police peuvent effectuer des contrôles de sécurité sur un employé afin de s'assurer que celui-ci est fiable pour accéder à des données de sécurité nationale. Bien que la police représente une autorité compétente à des fins répressives, le traitement en cause n'est pas effectué à ces fins et le RGPD britannique s'appliquerait. Voir le cadre explicatif relatif aux discussions sur l'adéquation du Royaume-Uni, section H: Cadre de la sécurité nationale, de la protection des données et des pouvoirs d'enquête, p. 8, disponible à l'adresse suivante: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf.

32 Article 2, paragraphe 1, points a) et b), du RGPD britannique.

33 Article 2, paragraphe 2, points b) et c), du RGPD britannique.

34 Le même champ d'application territorial s'applique au traitement de données à caractère personnel au titre de la partie 2 de la DPA 2018, qui complète le RGPD britannique (article 207, paragraphe 1A).

35 Cela signifie notamment que la DPA de 2018 et, par conséquent, la présente décision ne s'appliquent pas aux dépendances de la Couronne du Royaume-Uni (Jersey, Guernesey et île de Man) ni aux territoires d'outre-mer du Royaume-Uni, tels que les îles Falkland et le territoire de Gibraltar.

36 Article 4, paragraphes 1, 2, 5, 7 et 8, du RGPD britannique.

données visées à l'article 9, paragraphe 1, du RGPD britannique sont définies de la même manière que dans le règlement (UE) 2016/679 («données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique»). L'article 205 de la DPA 2018 donne la définition de «données biométriques»[37], de «données concernant la santé»[38] et de «données génétiques»[39].

2.5. Garanties, droits et obligations

2.5.1. Licéité et loyauté du traitement

(24) Les données à caractère personnel devraient être traitées de manière licite et loyale.

(25) Les principes de licéité, de loyauté et de transparence, ainsi que les fondements du traitement licite, sont garantis dans le droit du Royaume-Uni par les articles 5, paragraphe 1, point a), et 6, paragraphe 1, du RGPD britannique, lesquels sont identiques aux dispositions correspondantes du règlement (UE) 2016/679[40]. L'article 8 de la DPA 2018 complète l'article 6, paragraphe 1, point e), en prévoyant que le traitement de données à caractère personnel en vertu de l'article 6, paragraphe 1, point e) du RGPD britannique (nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement) inclut le traitement de données à caractère personnel nécessaire aux fins de l'administration de la justice, de l'exercice d'une fonction d'une des deux chambres du Parlement, de l'exercice d'une fonction conférée à une personne par une disposition législative ou une règle de droit, de l'exercice d'une fonction de la Couronne, d'un ministre de la Couronne ou d'un ministère, ou d'une activité qui soutient ou promeut l'engagement démocratique.

---

37 On entend par «données biométriques», les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques.

38 On entend par «données concernant la santé», les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne.

39 On entend par «données génétiques» les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question.

40 Conformément à l'article 6, paragraphe 1, du RGPD britannique, le traitement n'est licite que si, et dans la mesure où: a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques; b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci; c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis; d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique; e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement; ou f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

(26) En ce qui concerne le consentement (l'un des fondements du traitement licite), le RGPD britannique conserve également les conditions prévues à l'article 7 du règlement (UE) 2016/679 sans les modifier, à savoir les conditions suivantes: le responsable du traitement doit être en mesure de démontrer que la personne concernée a donné son consentement, une demande de consentement doit être formulée par écrit en des termes clairs et simples, la personne concernée doit avoir le droit de retirer son consentement à tout moment et, au moment de déterminer si le consentement est donné librement, il y a lieu de tenir compte de la question de savoir si l'exécution d'un contrat est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat. En outre, conformément à l'article 8 du RGPD britannique, dans le cadre de l'offre de services de la société de l'information, le consentement d'un enfant n'est licite que si ce dernier est âgé d'au moins 13 ans. Cet âge est compris dans la tranche d'âge déterminée à l'article 8 du règlement (UE) 2016/679.

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

(27) Des garanties spécifiques devraient être prévues pour le traitement des «catégories particulières» de données.

(28) Le RGPD britannique et la DPA 2018 contiennent des règles spécifiques concernant le traitement de catégories particulières de données à caractère personnel, lesquelles sont définies à l'article 9, paragraphe 1, du RGPD britannique de la même manière que dans le règlement (UE) 2016/679 [voir le considérant (23) above ci-dessus]. Conformément à l'article 9 du RGPD britannique, le traitement de catégories particulières de données est en principe interdit, à moins qu'une exception spécifique ne s'applique.

(29) Ces exceptions (énumérées à l'article 9, paragraphes 2 et 3, du RGPD britannique) n'apportent aucune modification de fond par rapport à celles figurant à l'article 9, paragraphes 2 et 3, du règlement (UE) 2016/679. À moins que la personne concernée n'ait donné son consentement explicite au traitement de ces données à caractère personnel, le traitement de catégories particulières de données à caractère personnel n'est autorisé que dans des circonstances particulières et limitées. Dans la plupart des cas, le traitement des données sensibles doit être nécessaire pour une finalité spécifique définie dans la disposition correspondante [voir l'article 9, paragraphe 2, points b), c), f), g), h), i) et j)].

(30) Par ailleurs, lorsqu'une exception prévue à l'article 9, paragraphe 2, du RGPD britannique nécessite une autorisation législative ou fait référence à l'intérêt public, l'article 10 de la DPA 2018, ainsi que son annexe 1, précisent plus en détail les conditions qui doivent être remplies pour invoquer ces exceptions. Par exemple, dans le cas du traitement de données sensibles aux fins de la protection de la «santé publique» (article 9, paragraphe 2, point i), du RGPD britannique), l'annexe 1, partie 1, point 3, sous b), prévoit que, outre le critère de nécessité, un tel traitement est effectué «par un professionnel de santé ou sous sa responsabilité» ou «par une autre personne qui est liée par une obligation de confidentialité en vertu d'une disposition législative ou d'une règle de droit», y compris par l'obligation de confidentialité bien établie dans la common law.

(31) Lorsque des données sensibles sont traitées pour des motifs d'intérêt public important [article 9, paragraphe 2, point g), du RGPD britannique], l'annexe 1, partie 2, de la DPA 2018 contient une liste exhaustive des finalités qui peuvent être considérées d'intérêt public important et prévoit, pour chacune de ces finalités, des conditions

spécifiques supplémentaires. Par exemple, la promotion de la diversité raciale et ethnique au sein de l'encadrement supérieur des organisations est reconnue comme étant d'intérêt public important. Le traitement de données sensibles pour cette finalité spécifique est soumis à des exigences détaillées, en particulier ce traitement doit être effectué dans le cadre d'un processus visant à désigner les personnes aptes à exercer des fonctions d'encadrement supérieur, doit être nécessaire à la promotion de la diversité raciale et ethnique et ne doit pas être susceptible de causer des difficultés ou des dommages importants à la personne concernée.

(32) L'article 11, paragraphe 1, de la DPA 2018 énonce les conditions applicables au traitement de données à caractère personnel dans les circonstances décrites à l'article 9, paragraphe 3, du RGPD britannique liées à l'obligation de secret. Sont incluses les circonstances dans lesquelles le traitement est effectué par un professionnel de la santé ou un professionnel social, ou sous sa responsabilité, ou par toute autre personne qui est liée par une obligation de confidentialité en vertu d'une disposition législative ou d'une règle de droit.

(33) En outre, beaucoup des exceptions énumérées à l'article 9, paragraphe 2, du RGPD britannique nécessitent des garanties appropriées et spécifiques pour être appliquées. En fonction de la nature du traitement et du niveau de risque pour les droits et libertés des personnes concernées, les conditions relatives au traitement prévues à l'annexe 1 de la DPA 2018 établissent des garanties différentes. L'annexe 1 décrit successivement les conditions applicables à chaque traitement.

(34) Dans certains cas, la DPA 2018 réglemente et limite le type de données sensibles qui peuvent être traitées aux fins du respect d'une base juridique particulière. Par exemple, l'annexe 1, point 8, autorise le traitement de données sensibles aux fins de la promotion de l'égalité des chances ou de traitement. Cette condition de traitement ne peut être invoquée que si les données révèlent l'origine raciale ou ethnique, les convictions religieuses ou philosophiques, l'orientation sexuelle ou s'il s'agit de données concernant la santé.

(35) Dans certains cas, la DPA 2018 limite le type de responsable du traitement qui peut invoquer la condition de traitement. Par exemple, l'annexe 1, point 23, prévoit le traitement de données sensibles dans le cadre de la réponse des élus aux demandes du public. Cette condition de traitement ne peut être invoquée que si le responsable du traitement est l'élu en question ou agit sous son autorité.

(36) Dans d'autres cas, la DPA 2018 fixe des limites concernant les catégories de personnes concernées aux fins de l'application de la condition de traitement. Par exemple, l'annexe 1, point 21, réglemente le traitement de données sensibles pour les régimes professionnels de retraite. Cette condition ne peut être invoquée que si la personne concernée est le frère, la sœur, le parent, le grand-parent ou l'arrière-grand-parent du membre du régime.

(37) En outre, lorsqu'il a recours aux exceptions prévues à l'article 9, paragraphe 2, du RGPD britannique, lesquelles sont précisées davantage à l'article 10 et à l'annexe 1 de la DPA 2018, le responsable du traitement est tenu, dans la plupart des cas, de rédiger un «document d'orientation spécifique». Ce dernier doit expliquer les procédures du responsable du traitement visant à garantir le respect des principes énoncés à l'article 5 du RGPD britannique. Il doit également décrire les politiques en matière de conservation et d'effacement, en indiquant la durée de conservation probable. Les responsables du traitement doivent revoir et mettre à jour ce document, le cas échéant. Le responsable du traitement doit conserver le document d'orientation pendant six

mois à compter de la fin du traitement et, sur demande, le mettre à la disposition du commissaire à l'information[41].

(38) Conformément à l'annexe 1, point 41, de la DPA 2018, le document d'orientation doit toujours s'accompagner d'un registre plus complet des activités de traitement. Ce registre doit permettre de suivre les engagements figurant dans le document d'orientation, c'est-à-dire de vérifier si les données sont effacées ou conservées conformément aux politiques du responsable du traitement. Si les politiques n'ont pas été respectées, le registre doit en indiquer les raisons. Le registre doit également indiquer la manière dont le traitement satisfait aux exigences de l'article 6 du RGPD britannique (licéité du traitement) et à la condition spécifique de l'annexe 1 de la DPA 2018 sur laquelle il se fonde.

(39) Enfin, comme le règlement (UE) 2016/679, le RGPD britannique prévoit également des garanties générales pour certaines opérations de traitement de catégories particulières de données. L'article 35 du RGPD britannique exige une analyse d'impact relative à la protection des données en cas de traitement à grande échelle de catégories particulières de données. Conformément à l'article 37 du RGPD britannique, un responsable du traitement ou un sous-traitant doit désigner un délégué à la protection des données lorsque ses activités de base consistent à traiter, à grande échelle, des catégories particulières de données.

(40) S'agissant des données à caractère personnel relatives à des condamnations pénales et à des infractions, l'article 10 du RGPD britannique est identique à l'article 10 du règlement (UE) 2016/679. Il n'autorise le traitement des données à caractère personnel relatives à des condamnations pénales et à des infractions que sous le contrôle de l'autorité publique, ou si le traitement est autorisé par le droit interne qui prévoit des garanties appropriées pour les droits et libertés des personnes concernées.

(41) Lorsque le traitement des données relatives à des condamnations pénales et à des infractions n'est pas effectué sous le contrôle de l'autorité publique, l'article 10, paragraphe 5, de la DPA 2018 dispose que ce traitement ne peut avoir lieu que pour les finalités spécifiques/dans les situations particulières visées à l'annexe 1, parties 1, 2 et 3, de la DPA 2018, et qu'il est soumis aux exigences spécifiques prévues pour chacune de ces finalités/situations. Par exemple, les données relatives à des condamnations pénales peuvent être traitées par des organismes à but non lucratif si le traitement est effectué a) dans le cadre de leurs activités légitimes et moyennant les garanties appropriées, par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale et b) à condition i) que ledit traitement se rapporte exclusivement aux membres ou aux anciens membres dudit organisme ou aux personnes entretenant avec celui-ci des contacts réguliers en liaison avec ses finalités et ii) que les données à caractère personnel ne soient pas communiquées en dehors de cet organisme sans le consentement des personnes concernées.

(42) Par ailleurs, l'annexe 1, partie 3, de la DPA 2018 décrit les autres circonstances dans lesquelles les données relatives à des condamnations pénales peuvent être utilisées, qui correspondent aux fondements juridiques du traitement de données sensibles visés à l'article 9, paragraphe 2, du règlement (UE) 2016/679 et du RGPD britannique (par exemple, consentement de la personne concernée, intérêts vitaux d'une personne si la

[41] Annexe 1, points 38 à 40, de la DPA 2018.

personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement, si les données ont déjà été manifestement rendues publiques par la personne concernée, si le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice, etc.).

2.5.3 Limitation des finalités, exactitude, minimisation des données, limitation de la conservation et sécurité des données

(43) Les données à caractère personnel doivent être traitées dans un but précis et n'être utilisées ultérieurement que dans la mesure où cela n'est pas incompatible avec la finalité du traitement.

(44) Ce principe est établi à l'article 5, paragraphe 1, point b), du règlement (UE) 2016/679 et a été conservé sans modifications à l'article 5, paragraphe 1, point b), du RGPD britannique. Les conditions applicables à un traitement ultérieur compatible conformément à l'article 6, paragraphe 4, du règlement (UE) 2016/679 ont également été conservées, sans modifications de fond, à l'article 6, paragraphe 4, points a) à e), du RGPD britannique.

(45) De plus, les données doivent être exactes et, si nécessaire, tenues à jour. Elles doivent également être adéquates, pertinentes et limitées au regard des finalités pour lesquelles elles sont traitées. Enfin, elles doivent en principe être conservées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.

(46) Ces principes de minimisation des données, d'exactitude et de limitation de la conservation sont énoncés à l'article 5, paragraphe 1, point c) à e), du règlement (UE) 2016/679 et sont conservés sans modifications à l'article 5, paragraphe 1, points c) à e), du RGPD britannique.

(47) Les données à caractère personnel devraient en outre être traitées d'une manière garantissant leur sécurité, y compris leur protection contre tout traitement non autorisé ou illicite et contre toute perte, toute destruction ou tout dégât d'origine accidentelle. À cette fin, les opérateurs économiques devraient prendre les mesures techniques ou organisationnelles appropriées pour protéger les données à caractère personnel contre d'éventuelles menaces. Ces mesures devraient être appréciées en fonction de l'état des connaissances et des coûts correspondants.

(48) La sécurité des données est consacrée dans le droit britannique par le principe d'intégrité et de confidentialité énoncé à l'article 5, paragraphe 1, point f), du RGPD britannique et à son article 32 relatif à la sécurité du traitement. Ces dispositions sont identiques aux dispositions correspondantes du règlement (UE) 2016/679. Par ailleurs, le RGPD britannique impose la notification à l'autorité de contrôle d'une violation de données à caractère personnel (article 33) et la communication à la personne concernée d'une violation de données à caractère personnel (article 34) dans les mêmes conditions que celles énoncées aux articles 33 et 34 du règlement (UE) 2016/679.

2.5.4 Transparence

(49) Les personnes concernées devraient être informées des principales caractéristiques du traitement des données à caractère personnel les concernant.

(50) Ce principe est garanti par les articles 13 et 14 du RGPD britannique qui, outre un principe général de transparence, établissent les règles relatives aux informations à fournir aux personnes concernées[42]. Le RGPD britannique n'apporte aucune modification de fond à ces règles par rapport aux articles correspondants du règlement (UE) 2016/679. Toutefois, comme dans le règlement (UE) 2016/679, les exigences de transparence de ces articles font l'objet de plusieurs exceptions prévues par la DPA 2018 [voir les considérants (55) à (72)].

2.5.5 Droits individuels

(51) Les personnes concernées devraient disposer de certains droits qu'elles peuvent opposer au responsable du traitement ou au sous-traitant, en particulier le droit d'accéder aux données, le droit de s'opposer au traitement et le droit d'obtenir la rectification et l'effacement des données. Dans le même temps, de tels droits peuvent être soumis à des limitations, dans la mesure où celles-ci sont nécessaires et proportionnées pour garantir la sécurité publique ou d'autres objectifs d'intérêt public importants.

2.5.5.1 Les droits substantiels

(52) Le RGPD britannique confère aux personnes physiques les mêmes droits opposables que ceux prévus par le règlement (UE) 2016/679. Les dispositions établissant les droits des personnes ont été maintenues dans le RGPD britannique sans modifications de fond.

(53) Ces droits incluent le droit d'accès de la personne concernée (article 15 du RGPD britannique), le droit de rectification (article 16 du RGPD britannique), le droit à l'effacement (article 17 du RGPD britannique), le droit à la limitation du traitement (article 18 du RGPD britannique), une obligation de notification en ce qui concerne la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement (article 19 du RGPD britannique), le droit à la portabilité des données (article 20 du RGPD britannique) et le droit d'opposition (article 21 du RGPD britannique)[43]. Ce dernier comprend le droit d'une personne concernée de s'opposer au traitement des données à caractère personnel à des fins de prospection, conformément

---

42 Dans les articles 13, paragraphe 1, point f), et 14, paragraphe 1, point f), les références aux décisions d'adéquation de la Commission ont été remplacées par des références à l'instrument britannique équivalent, à savoir les règlements d'adéquation au titre de la DPA 2018. Par ailleurs, dans les articles 14, paragraphe 5, points c) et d), les références au droit de l'Union ou au droit des États membres ont été remplacées par une référence au droit interne [le Royaume-Uni a mentionné, à titre d'exemple d'une telle législation nationale susceptible de relever de l'article 14, paragraphe 5, point c), l'article 7 de la loi de 2013 sur les ferrailleurs qui fixe les règles relatives au registre des licences de ferrailleurs, ou la partie 35 de la loi de 2006 sur les sociétés énonçant les règles applicables au registre des sociétés. De même, on peut citer à titre d'exemple de législation nationale susceptible de relever de l'article 14, paragraphe 5, point d), la législation établissant les règles relatives au secret professionnel, les obligations figurant dans les contrats de travail ou l'obligation de confidentialité imposée par la *common law* (comme dans le cas du traitement de données à caractère personnel par des professionnels de la santé, les ressources humaines, les travailleurs sociaux, etc.).

43 Dans l'article 17, paragraphe 1, point e) et paragraphe 3, point b), les références au droit de l'Union et au droit des États membres ont été remplacées par une référence au droit national [le Royaume-Uni a mentionné, à titre d'exemple d'une telle législation nationale relevant de l'article 17, paragraphe 1, point e), la réglementation de 2006 sur l'éducation (information concernant les élèves) (Angleterre) en vertu de laquelle le nom des élèves doit être effacé des registres scolaires après leur départ de l'école, ou la loi médicale de 1983, article 34F, qui fixe les règles relatives à la suppression des noms dans le registre des médecins généralistes et le registre des médecins spécialistes].

à l'article 21, paragraphes 2 et 3, du règlement (UE) 2016/679. De plus, en vertu de l'article 122 de la DPA 2018, le commissaire à l'information doit préparer un code de bonnes pratiques relatif à l'exercice des activités de prospection dans le respect des exigences de la législation en matière de protection des données [et de la réglementation de 2003 sur la vie privée et les communications électroniques (directive CE)], ainsi que d'autres orientations afin de promouvoir les bonnes pratiques de prospection qu'il juge appropriées. Le bureau du commissaire à l'information élabore actuellement le code relatif à la prospection[44].

(54) Le droit de la personne concernée de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé et produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire, tel qu'il est prévu à l'article 22 du RGPD, a également été conservé dans le RGPD britannique sans modifications de fond. Cependant, un nouveau paragraphe 3A a été ajouté afin de mentionner que l'article 14 de la DPA 2018 prévoit des garanties pour les droits, les libertés et les intérêts légitimes des personnes concernées lorsque le traitement est effectué au titre de l'article 22, paragraphe 2, point b), du RGPD britannique. L'article 14 ne s'applique que lorsqu'une telle décision est autorisée ou requise en vertu du droit britannique et ne s'applique pas lorsque la décision est requise en vertu d'un contrat ou lorsqu'elle est prise avec le consentement explicite de la personne concernée. Lorsque l'article 14 de la DPA 2018 s'applique, le responsable du traitement doit, dès que cela est raisonnablement possible, notifier par écrit à la personne concernée qu'une décision a été prise sur le seul fondement d'un traitement automatisé. La personne concernée a le droit de demander que le responsable du traitement, dans un délai d'un mois à compter de la réception de la notification, réexamine la décision ou prenne une nouvelle décision qui ne soit pas fondée exclusivement sur un traitement automatisé. Le secrétaire d'État est habilité à adopter des garanties supplémentaires en ce qui concerne la prise de décision automatisée. Ce pouvoir n'a pas encore été exercé.

2.5.5.2 Limitations des droits individuels et autres dispositions

(55) La DPA 2018 prévoit plusieurs limitations des droits individuels, qui s'inscrivent dans le cadre de l'article 23 du RGPD britannique. Aucune limitation n'est introduite dans ce cadre en ce qui concerne le droit de s'opposer à la prospection, tel qu'il est prévu à l'article 21, paragraphes 2 et 3, du RGPD britannique, ou le droit de ne pas faire l'objet d'une prise de décision automatisée, tel qu'il est prévu à l'article 22 du RGPD britannique.

(56) Ces limitations sont détaillées aux annexes 2 à 4 de la DPA 2018. Les autorités britanniques ont expliqué qu'elles étaient guidées par deux principes: le principe de spécificité (adoption d'une approche granulaire, en divisant des limitations générales en plusieurs dispositions plus spécifiques) et le principe de conditionnalité (chaque disposition est complétée par des garanties sous la forme de limitations ou de conditions afin d'éviter les abus)[45].

---

44 Le projet de code de bonnes pratiques est disponible à l'adresse suivante: https://ico.org.uk/media/about-the-ico/consultations/2616882/direct-marketing-code-draft-guidance.pdf

45 Cadre explicatif relatif aux discussions sur l'adéquation du Royaume-Uni, section E: Limitations, p. 1, disponible à l'adresse suivante: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf.

(57) Les limitations décrites à l'article 23, paragraphe 1, du RGPD britannique visent à faire en sorte qu'elles ne soient appliquées que dans des circonstances déterminées, lorsqu'elles sont nécessaires dans une société démocratique et proportionnées à l'objectif légitime poursuivi. En outre, conformément à la jurisprudence constante au sujet de l'interprétation des limitations, une exemption du régime de protection des données ne peut être appliquée dans un cas d'espèce que si elle est nécessaire et proportionnée[46]. Le critère de nécessité doit être «strict et exiger que toute ingérence dans les droits de la personne soit proportionnée à la gravité de la menace pour l'intérêt public. Cet exercice nécessite donc une analyse de proportionnalité classique[47]».

(58) Les finalités visées par ces limitations correspondent à celles énumérées à l'article 23 du règlement (UE) 2016/679, sauf en ce qui concerne les limitations relatives à la sécurité nationale et à la défense, lesquelles sont plutôt réglementées par l'article 26 de la DPA 2018. Toutefois, elles sont soumises aux mêmes exigences de nécessité et de proportionnalité [voir les considérants (63) à (66)].

(59) Certaines de ces limitations, par exemple celles relatives à la prévention ou à la détection des infractions pénales, à l'arrestation ou à la poursuite des criminels et à l'établissement ou au recouvrement d'un impôt, d'une taxe ou d'un droit[48], permettent de restreindre l'ensemble des droits individuels et des obligations de transparence (à l'exclusion des droits prévus à l'article 21, paragraphe 2, et à l'article 22). La portée des autres limitations est limitée aux obligations de transparence et aux droits d'accès, comme celles relatives au secret professionnel[49], au droit d'être dégagé de l'obligation de fournir des informations qui conduiraient à s'auto-incriminer[50], et au financement des entreprises, notamment la prévention des délits d'initiés[51]. Quelques limitations permettent de restreindre l'obligation, pour le responsable du traitement, de communiquer une violation de données à une personne concernée et les principes de limitation de la finalité, de licéité, de loyauté et de transparence du traitement[52].

(60) Certaines de ces limitations s'appliquent automatiquement et «pleinement» à un certain type de traitement de données à caractère personnel (par exemple, l'application des obligations de transparence et des droits individuels est exclue lorsque les données à caractère personnel sont traitées afin d'évaluer l'aptitude d'une personne à exercer une fonction juridictionnelle ou lorsqu'elles sont traitées par une juridiction ou par une personne agissant dans l'exercice d'une fonction juridictionnelle).

---

46 Arrêt dans l'affaire Open Rights Group et Anor, R (On the Application Of)/Secretary of State for the Home Department et Anor [2019] EWHC 2562 (Admin), points 40 et 41.

47 Arrêt dans l'affaire Guriev/Community Safety Development (UK) Ltd [2016] EWHC 643 (QB), point 43. Voir également à ce sujet l'arrêt dans l'affaire Lin/Commissioner of Police for the Metropolis [2015] EWHC 2484 (QB), point 80.

48 Annexe 2, point 2, de la DPA 2018.

49 Annexe 2, point 19, de la DPA 2018.

50 Annexe 2, point 20, de la DPA 2018.

51 Annexe 2, point 21, de la DPA 2018.

52 Par exemple, les limitations du droit à la notification d'une violation de données ne sont autorisées qu'en ce qui concerne la criminalité et la fiscalité (annexe 2, point 2, de la DPA 2018), l'immunité parlementaire (annexe 2, point 13, de la DPA 2018) et le traitement à des fins journalistiques, universitaires, artistiques et littéraires (annexe 2, point 26, de la DPA 2018).

(61) Cependant, dans la majorité des cas, le point pertinent de l'annexe 2 de la DPA 2018 précise que la limitation ne s'applique que lorsque (et dans la mesure où) l'application des dispositions «est susceptible de porter préjudice» à l'objectif légitime poursuivi par cette limitation: par exemple, les dispositions énumérées dans le RGPD britannique ne s'appliquent pas aux données à caractère personnel traitées aux fins de la prévention ou de la détection des infractions pénales, de l'arrestation ou de la poursuite des criminels, ou de l'établissement ou du recouvrement d'un impôt, d'une taxe ou d'un droit «dans la mesure où l'application de ces dispositions est susceptible de porter préjudice» à ces finalités, quelles qu'elles soient[53].

(62) Le critère de «préjudice probable» a été systématiquement interprété par les tribunaux britanniques comme «un risque très significatif et important de porter préjudice aux intérêts généraux visés»[54]. Une restriction soumise au critère du préjudice ne peut donc être invoquée que si et dans la mesure où il existe une probabilité très importante et importante que l'octroi d'un certain droit porterait atteinte à l'intérêt public en jeu. Le responsable du traitement est chargé d'évaluer au cas par cas si ces conditions sont remplies[55].

(63) Outre les limitations visées à l'annexe 2 de la DPA 2018, son article 26 prévoit une exemption qui peut s'appliquer à certaines dispositions du RGPD britannique et de la DPA 2018 si celle-ci est nécessaire pour garantir la sécurité nationale ou à des fins de défense. Cette exemption s'applique aux principes relatifs à la protection des données (à l'exception du principe de licéité), aux obligations de transparence, aux droits de la personne concernée, à l'obligation de notifier une violation de données, aux règles relatives aux transferts internationaux, à certains des devoirs et des pouvoirs du commissaire à l'information et aux règles relatives aux voies de recours, à la responsabilité et aux sanctions, à l'exception de la disposition de l'article 83 du RGPD britannique relative aux conditions générales applicables à l'imposition d'amendes administratives et de la disposition de son article 84 relative aux sanctions. En outre, l'article 28 de la DPA 2018 modifie l'application de l'article 9, paragraphe 1, du RGPD britannique afin de permettre le traitement des catégories particulières de données énoncées dans cet article, dans la mesure où le traitement est effectué pour garantir la sécurité nationale ou à des fins de défense, moyennant les garanties appropriées pour les droits et libertés des personnes concernées[56].

(64) L'exemption ne peut être appliquée que dans la mesure où elle est nécessaire pour garantir la sécurité nationale ou la défense. De la même manière que pour les autres exemptions prévues par la DPA 2018, elle doit être envisagée et invoquée par le

---

53 Annexe 2, point 2, de la DPA 2018.

54 Arrêt dans l'affaire R (Lord)/Secretary of State for the Home Department [2003] EWHC 2073 (Admin), point 100, et arrêt dans l'affaire Guriev/Community Safety Development (UK) Ltd [2016] EWHC 643 (QB), point 43.

55 Arrêt dans l'affaire Open Rights Group et Anor, R (On the Application Of)/Secretary of State for the Home Department et Anor, point 31.

56 Selon les informations fournies par les autorités britanniques, lorsque le traitement s'inscrit dans le cadre de la sécurité nationale, les responsables du traitement appliqueront généralement des garanties et des mesures de sécurité renforcées, reflétant la nature sensible du traitement. La détermination des garanties appropriées dépendra des risques posés par le traitement entrepris. Ces garanties pourraient inclure des restrictions d'accès aux données afin que seules les personnes autorisées disposant d'une habilitation de sécurité appropriée puissent y accéder, des restrictions strictes concernant le partage des données et l'application d'une norme de sécurité élevée aux procédures de conservation et de traitement.

responsable du traitement au cas par cas. 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), selon lesquelles toute ingérence dans les droits au respect de la vie privée devrait être nécessaire et proportionnée dans une société démocratique[57].

(65) Cette interprétation de l'exemption est confirmée par l'ICO, qui a publié des orientations détaillées sur l'application de l'exemption en matière de sécurité et de défense nationales, indiquant clairement qu'elle doit être examinée et appliquée par le responsable du traitement au cas par cas[58]. En particulier, les orientations soulignent que «le traitement des données n'est pas une exemption générale» et que, pour l'invoquer, «il ne suffit pas que les données soient traitées à des fins de sécurité nationale». En revanche, le responsable du traitement qui l'invoque doit «démontrer qu'il existe une possibilité réelle d'atteinte à la sécurité nationale» et, le cas échéant, il est censé «fournir [à l'ICO] des éléments de preuve sur les raisons pour lesquelles il a eu recours à cette exemption». Les orientations contiennent une liste de contrôle et une série d'exemples visant à clarifier davantage les conditions dans lesquelles cette exemption peut être invoquée.

(66) Le fait que les données soient traitées à des fins de sécurité nationale ou de défense ne suffit donc pas en soi pour appliquer l'exemption. Un responsable du traitement doit considérer les conséquences concrètes pour la sécurité nationale s'il devait respecter la disposition particulière relative à la protection des données. L'exemption ne peut s'appliquer qu'aux dispositions spécifiques qui ont été désignées comme posant un tel risque et cette application doit être aussi restrictive que possible[59].

(67) Cette approche a été confirmée par le tribunal de l'information (*Information Tribunal*)[60]. Dans l'arrêt Baker/Secretary of State for the Home Department (ci-après l'«arrêt Baker/Secretary of State»), ce tribunal a déterminé qu'il était illégal

---

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

58 Voir les orientations d'ICO sur l'exception en matière de sécurité et de défense nationales, disponibles à l'adresse suivante: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national-security-and-defence/

59 Selon un exemple fourni par les autorités britanniques, si un terroriste présumé faisant l'objet d'une enquête active menée par le MI5 introduisait une demande d'accès auprès du ministère de l'intérieur (par exemple, parce qu'il est en désaccord avec celui-ci sur des questions d'immigration), il serait nécessaire d'empêcher la communication à la personne concernée de toutes les données que le MI5 est susceptible d'avoir partagées avec le ministère de l'intérieur concernant des enquêtes en cours et qui pourraient porter préjudice à des sources, à des méthodes ou à des techniques sensibles et/ou accroître la menace que représente cet individu. Dans de telles circonstances, il est probable que le seuil d'application de l'exemption prévue à l'article 26 soit atteint et qu'une exemption de la communication des informations soit nécessaire pour garantir la sécurité nationale. Toutefois, si le ministère de l'intérieur détenait également des données à caractère personnel concernant la personne physique qui n'étaient pas liées à l'enquête du MI5 et si ces informations pouvaient être communiquées sans risquer de compromettre la sécurité nationale, l'exemption concernant la sécurité nationale ne serait pas applicable pour ce qui est de leur communication à la personne. L'ICO prépare actuellement des orientations sur la manière dont les responsables du traitement devraient envisager d'utiliser l'exemption prévue à l'article 26. Ces orientations devraient être publiées d'ici la fin du mois de mars 2021.

60 Le tribunal de l'information a été institué pour connaître des recours en matière de protection des données par la loi de 1984 sur la protection des données. En 2010, le tribunal de l'information a été intégré à la division de la réglementation générale du tribunal de première instance, dans le cadre de la réforme de la structure du système de tribunaux au Royaume-Uni.

d'appliquer l'exemption concernant la sécurité nationale comme une exemption générale aux demandes d'accès reçues par les services de renseignement. L'exemption doit plutôt être appliquée au cas par cas, en examinant le bien-fondé de chaque demande et en tenant compte du droit des personnes au respect de leur vie privée[61].

2.5.6 Limitations concernant le traitement des données à caractère personnel réalisé à des fins journalistiques, artistiques, universitaires et littéraires, ainsi qu'à des fins archivistiques et de recherche

(68) L'article 85, paragraphe 2, du RGPD britannique permet de prévoir des exemptions à plusieurs de ses dispositions pour le traitement des données à caractère personnel réalisé à des fins journalistiques, artistiques, universitaires et littéraires. L'annexe 2, partie 5, de la DPA 2018 définit les exemptions applicables au traitement effectué à ces fins. Elle prévoit des exemptions aux principes relatifs à la protection des données (à l'exception du principe d'intégrité et de confidentialité), aux fondements juridiques du traitement (y compris pour les catégories particulières de données, les données relatives à des condamnations pénales, etc.), aux conditions applicables au consentement, aux obligations de transparence, aux droits des personnes concernées, à l'obligation de notifier une violation de données, à l'obligation de consulter le commissaire à l'information avant un traitement présentant un risque élevé et aux règles relatives aux transferts internationaux[62]. À cet égard, le RGPD britannique ne s'écarte pas de manière substantielle du règlement (UE) 2016/679, lequel, dans son article 85, prévoit également la possibilité d'exempter le traitement réalisé à des fins journalistiques ou à des fins d'expression universitaire, artistique ou littéraire de plusieurs exigences dudit règlement. Les dispositions de la DPA 2018, notamment son annexe 2, partie 5, sont compatibles avec le RGPD britannique.

(69) L'exercice de mise en balance fondamental à effectuer au titre de l'article 85 du RGPD britannique porte sur la question de savoir si une exemption aux règles en matière de protection des données mentionnées au considérant (68) est «nécessaire pour concilier le droit à la protection des données à caractère personnel et la liberté d'expression et d'information»[63]. Conformément à l'annexe 2, point 26, sous 2) et 3), de la DPA 2018, le Royaume-Uni applique le critère de la «croyance raisonnable» en vue de trouver cet équilibre. Pour qu'une exemption soit justifiée, le responsable du traitement doit raisonnablement croire i) que la publication est d'intérêt public; et ii) que l'application de la disposition pertinente du RGPD serait incompatible avec les finalités journalistiques, universitaires, artistiques ou littéraires. Comme le confirme la

61 Voir l'arrêt Baker/Secretary of State for the Home Department [2001] UKIT NSA2 (ci-après l'«arrêt Baker/Secretary of State»).

62 Voir l'article 85 du RGPD britannique et l'annexe 2, partie 5, paragraphe 26, point 9), de la DPA 2018.

63 Conformément à l'annexe 2, partie 5, point 26, sous 2), de la DPA 2018, l'exception s'applique au traitement de données à caractère personnel réalisé à des fins particulières (à des fins journalistiques, universitaires, artistiques ou littéraires) en vue de la publication par une personne de contenus de nature journalistique, universitaire, artistique ou littéraire, lorsque le responsable du traitement croit raisonnablement que la publication de ce contenu serait d'intérêt public. Pour déterminer si une publication serait ou non d'intérêt public, le responsable du traitement doit prendre en compte l'importance particulière que revêt l'intérêt public eu égard à la liberté d'expression et d'information. En outre, il doit tenir compte des directives ou des codes de bonnes pratiques applicables à la publication en question (directives éditoriales de la BBC, code de diffusion de l'Ofcom et code de bonnes pratiques entre éditeurs). En outre, pour qu'une exemption puisse s'appliquer le responsable du traitement doit raisonnablement croire que le respect de la disposition pertinente serait incompatible avec les finalités particulières [annexe 2, point 26, sous 3), de la DPA 2018].

jurisprudence[64], le critère de la «croyance raisonnable» comporte à la fois un élément subjectif et objectif: il ne suffit pas, pour le responsable du traitement, de démontrer qu'il croyait personnellement que le respect de la disposition était incompatible. Sa croyance doit être raisonnable, c'est-à-dire qu'elle pourrait être partagée par une personne raisonnable ayant connaissance des faits pertinents. Par conséquent, le responsable du traitement doit faire preuve d'un soin particulier lorsqu'il se forge une croyance afin d'être en mesure de démontrer son caractère raisonnable. D'après les explications fournies par les autorités du Royaume-Uni, le critère de la «croyance raisonnable» doit être appliqué au cas par cas[65]. Si les conditions sont remplies, l'exemption est considérée comme nécessaire et proportionnée en vertu du droit britannique.

(70) Conformément à l'article 124 de la DPA 2018, l'ICO doit préparer un code de bonnes pratiques relatif à la protection des données et au journalisme. Ce code est en cours d'élaboration. Les orientations publiées sur la question relevant de la loi de 1998 sur la protection des données soulignent notamment que, pour appliquer cette exemption, il ne suffit pas d'affirmer que le respect de la disposition entraverait les activités journalistiques, mais il faut également démontrer clairement que la disposition en cause constitue un obstacle au journalisme responsable[66]. Des orientations relatives à l'application du critère de l'intérêt public et à la mise en balance de l'intérêt public avec le droit au respect de la vie privée d'une personne ont également été publiées par l'autorité de régulation des télécommunications du Royaume-Uni, l'Ofcom, et par la BBC dans ses directives éditoriales[67]. Les directives fournissent notamment des

64 L'arrêt dans l'affaire NT1/Google [2018] EWHC 799 (QB), point 102, a clos le débat sur la question de savoir si le responsable du traitement avait des raisons de croire que la publication était d'intérêt public et que le respect des dispositions pertinentes était incompatible avec les finalités particulières. La cour a déclaré que l'article 32, paragraphe 1, points b) et c), de la loi de 1998 sur la protection des données comportait à la fois un élément subjectif et objectif: le responsable du traitement doit démontrer qu'il croyait que la publication serait d'intérêt public, et que cette croyance était objectivement raisonnable; il doit également établir sa croyance subjective selon laquelle le respect de la disposition pour laquelle il souhaite obtenir une exemption serait incompatible avec la finalité particulière en question.

65 On trouve un exemple de l'application du critère de la «croyance raisonnable» dans la décision de l'ICO d'infliger une amende à *True Visions Productions*, prise en vertu de la loi de 1998 sur la protection des données. L'ICO a reconnu la croyance subjective du contrôleur des médias selon laquelle le respect du premier principe de protection des données (loyauté et licéité) était incompatible avec les finalités journalistiques. Toutefois, il n'a pas reconnu que cette croyance était objectivement raisonnable. La décision de l'ICO est disponible à l'adresse suivante: https://ico.org.uk/media/action-weve-taken/mpns/2614746/true-visions-productions-20190408.pdf

66 Conformément aux orientations, les organisations doivent être en mesure d'expliquer les raisons pour lesquelles le respect de la disposition pertinente de la loi de 1998 sur la protection des données est incompatible avec les finalités du journalisme. Les responsables du traitement doivent notamment mettre en balance l'effet néfaste que le respect de la disposition aurait sur le journalisme avec celui que le non-respect de la disposition aurait sur les droits de la personne concernée. Si un journaliste peut raisonnablement atteindre ses objectifs éditoriaux d'une manière conforme aux dispositions générales de la loi sur la protection des données, il doit procéder de cette manière. Les organisations doivent être en mesure de justifier leur recours à la limitation pour toutes les dispositions qu'elles n'ont pas respectées. «Data protection and journalism: a guide for the media», disponible à l'adresse suivante: https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf.

67 Parmi les exemples de motifs d'intérêt public figurent la dénonciation ou la détection d'infractions pénales, la protection de la santé ou de la sécurité publique, la révélation de déclarations trompeuses faites par des personnes ou des organisations ou la révélation d'incompétences ayant des conséquences pour le public. Voir les orientations de l'Ofcom, disponibles à l'adresse suivante:

exemples d'informations pouvant être considérées comme relevant de l'intérêt public, et expliquent la nécessité d'être en mesure de démontrer la supériorité de l'intérêt public sur le droit au respect de la vie privée dans les circonstances particulières du cas en question.

(71) À l'instar de ce que prévoit l'article 89 du RGPD, les données à caractère personnel traitées à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques peuvent également être exemptées d'un certain nombre de dispositions énumérées dans le RGPD britannique[68]. En ce qui concerne les finalités de recherche et statistiques, des exemptions sont possibles aux dispositions du RGPD britannique relatives à la confirmation du traitement et à l'accès aux données et aux garanties pour les transferts vers des pays tiers; le droit de rectification; le droit à la limitation du traitement et à l'opposition au traitement. S'agissant des finalités archivistiques dans l'intérêt public, des exemptions sont également possibles à l'obligation de notification liée à la rectification ou à l'effacement de données à caractère personnel ou à la limitation du traitement, ainsi qu'au droit à la portabilité des données.

(72) Conformément à l'annexe 2, point 27, sous 1), et point 28, sous 1), de la DPA 2018, les exemptions aux dispositions énumérées dans le RGPD britannique sont possibles lorsque l'application de ces dispositions «rendrait impossible ou compromettrait gravement la réalisation» des finalités en cause[69].

(73) Compte tenu de leur importance pour l'exercice effectif des droits individuels, toute évolution pertinente concernant l'interprétation et l'application pratique des exemptions susmentionnées (en plus de celle relative au maintien d'un contrôle efficace de l'immigration, comme expliqué au considérant 6), y compris toute évolution ultérieure de la jurisprudence et des orientations et mesures d'exécution de l'ICO, sera dûment prise en compte dans le cadre du suivi continu de la présente décision[70].

2.5.7 Limitations concernant les transferts ultérieurs

(74) Le niveau de protection conféré aux données à caractère personnel qui sont transférées depuis l'Union européenne vers des responsables du traitement ou des sous-traitants au Royaume-Uni ne doit pas être compromis par le transfert ultérieur de ces mêmes données vers des destinataires se trouvant dans un pays tiers. Ces «transferts ultérieurs» qui constituent, du point de vue du responsable du traitement ou du sous-traitant britannique, des transferts internationaux en provenance du Royaume-Uni ne devraient être autorisés que si le destinataire ultérieur en dehors du Royaume-Uni est lui-même soumis à des règles assurant un niveau de protection semblable à celui garanti par l'ordre juridique britannique. C'est pourquoi l'application des règles du RGPD britannique et de la DPA 2018 relatives aux transferts internationaux de

---

https://www.ofcom.org.uk/__data/assets/pdf_file/0017/132083/Broadcast-Code-Section-8.pdf et les directives éditoriales de la BBC disponibles à l'adresse suivante: https://www.bbc.com/editorialguidelines/guidelines/privacy.

68 Voir l'article 89 du RGPD britannique et l'annexe 2, partie 6, point 27, sous 2), et point 28, sous 2), de la DPA 2018.

69 Ces exemptions sont subordonnées à la condition que les données à caractère personnel soient traitées conformément à l'article 89, paragraphe 1, du RGPD britannique, complété par l'article 19 de la DPA 2018.

70 Voir les considérants (281) à (287).

données à caractère personnel est un facteur important pour garantir la continuité de la protection en cas de transfert de données à caractère personnel au départ de l'Union européenne vers le Royaume-Uni en vertu de la présente décision.

(75) Le régime applicable aux transferts internationaux de données à caractère personnel en provenance du Royaume-Uni est décrit aux articles 44 à 49 du RGPD britannique, complétés par la DPA 2018, et est, en substance, identique aux règles définies au chapitre V du règlement (UE) 2016/679[71]. Les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale ne peuvent avoir lieu que sur le fondement d'un règlement d'adéquation [l'équivalent au Royaume-Uni d'une décision d'adéquation en vertu du règlement (UE) 2016/679] ou, en l'absence d'un tel règlement, lorsque le responsable du traitement ou le sous-traitant a prévu des garanties appropriées conformément à l'article 46 du RGPD britannique. En l'absence d'un règlement d'adéquation ou de garanties appropriées, un transfert ne peut avoir lieu que sur la base des dérogations prévues à l'article 49 du RGPD britannique.

(76) Les règlements d'adéquation adoptés par le secrétaire d'État peuvent disposer qu'un pays tiers (ou un territoire ou un secteur dans un pays tiers), une organisation internationale ou une description[72] de ce pays, de ce territoire, de ce secteur ou de cette organisation assure un niveau adéquat de protection des données à caractère personnel. Lorsqu'il évalue le caractère adéquat du niveau de protection, le secrétaire d'État doit tenir compte exactement des mêmes éléments que ceux que la Commission est tenue d'apprécier au titre de l'article 45, paragraphe 2, points a) à c), du

---

71 À l'exception de l'article 48 du règlement (UE) 2016/679 que le Royaume-Uni a décidé de ne pas inclure dans le RGPD britannique. À cet égard, il convient tout d'abord de rappeler que le critère devant être considéré comme assurant un niveau de protection adéquat est un critère d'«équivalence essentielle» plutôt que d'identité, comme l'a précisé la CJUE (arrêt Schrems I, points 73 et 74) et reconnu par le comité européen de la protection des données (Critères de référence pour l'adéquation, page 3). Par conséquent, comme l'a expliqué le comité européen de la protection des données dans sa référence relative à l'adéquation, «l'objectif n'est pas de refléter point par point la législation européenne, mais d'établir les exigences essentielles de cette législation». À cet égard, il est important de noter que, bien que l'ordre juridique britannique ne contienne pas formellement une disposition identique à l'article 48, le même effet est garanti par d'autres dispositions et principes juridiques, à savoir qu'en réponse à une demande de données à caractère personnel émanant d'une juridiction ou d'une autorité administrative d'un pays tiers, les données à caractère personnel ne peuvent être transférées vers ce pays tiers que s'il existe un accord international en vigueur — sur la base duquel la décision judiciaire ou la décision administrative du pays tiers en question est reconnue ou exécutée au Royaume-Uni — ou s'il est fondé sur l'un des mécanismes de transfert définis au chapitre V du RGPD britannique.

Plus précisément, pour exécuter une décision étrangère, les juridictions du Royaume-Uni doivent être en mesure de se fonder sur la common law ou une loi qui permet son opposabilité. Toutefois, ni la common law (voir *Adams and Others* v *Cape Industries Plc.*, [1990] 2 W.L.R. 657) ni le droit écrit ne prévoient l'exécution des décisions étrangères exigeant le transfert de données en l'absence d'un accord international. En conséquence, les demandes de transfert de données ne sont pas exécutoires en vertu du droit britannique, en l'absence d'un tel accord international. En outre, tout transfert de données à caractère personnel vers des pays tiers — y compris à la demande d'une juridiction ou d'une autorité administrative étrangère — reste soumis aux restrictions énoncées au chapitre V du RGPD britannique, qui sont identiques aux dispositions correspondantes du règlement (UE) 2016/679, et exige donc de se fonder sur l'un des motifs de transfert prévus au chapitre V conformément aux conditions spécifiques auxquelles il est soumis en vertu dudit chapitre.

72 Les autorités britanniques ont expliqué que la description d'un pays ou d'une organisation internationale faisait référence à une situation dans laquelle il serait nécessaire de procéder à une détermination spécifique et partielle du caractère adéquat avec des limitations ciblées (par exemple, un règlement d'adéquation qui ne concernerait que certains types de transferts de données).

règlement (UE) 2016/679, interprété en combinaison avec son considérant 104 et la jurisprudence de l'UE conservée. Autrement dit, lors de l'évaluation du caractère adéquat du niveau de protection d'un pays tiers, le critère pertinent consistera à déterminer si ce pays tiers assure un niveau de protection «essentiellement équivalent» à celui qui est garanti au Royaume-Uni.

(77) S'agissant de la procédure, les règlements d'adéquation sont soumis aux règles de procédure «générales» prévues à l'article 182 de la DPA 2018. 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[73]. 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[74].

(78) Conformément à l'article 17B, paragraphe 1, de la DPA 2018, les règlements d'adéquation doivent être réexaminés au moins tous les quatre ans et le secrétaire d'État doit suivre, de manière permanente, les évolutions dans les pays tiers et au sein des organisations internationales qui pourraient affecter les décisions d'adopter, de modifier ou d'abroger ces règlements. Lorsque le secrétaire d'État constate qu'une organisation ou un pays donné n'assure plus un niveau de protection adéquat des données à caractère personnel, il doit, dans la mesure nécessaire, modifier ou abroger les règlements et engager des consultations avec l'organisation internationale ou le pays tiers concerné afin de remédier à l'insuffisance du niveau de protection. Ces aspects de la procédure reflètent également les exigences correspondantes du règlement (UE) 2016/679.

(79) En l'absence de règlement d'adéquation, les transferts internationaux peuvent avoir lieu lorsque le responsable du traitement ou le sous-traitant a prévu des garanties appropriées conformément à l'article 46 du RGPD britannique. Ces garanties sont semblables à celles visées à l'article 46 du règlement (UE) 2016/679. Elles comprennent des instruments juridiquement contraignants et exécutoires entre les autorités ou organismes publics, des règles d'entreprise contraignantes[75], des clauses types de protection des données, des codes de conduite approuvés, des mécanismes de certification approuvés et, sous réserve de l'autorisation du commissaire à l'information, des clauses contractuelles entre les responsables du traitement (ou les sous-traitants) ou des arrangements administratifs entre les autorités publiques. Toutefois, les règles ont été modifiées, du point de vue de la procédure, pour fonctionner dans le cadre du Royaume-Uni. En particulier, les clauses types de

---

73 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.

74 Si une telle motion est adoptée, les règlements cesseront à terme de produire tout autre effet juridique.

75 Le RGPD britannique conserve les règles prévues à l'article 47 du règlement (UE) 2016/679, et se contente de les modifier afin de les adapter au contexte national, en remplaçant par exemple la référence à l'autorité de contrôle compétente par une référence au commissaire à l'information, en supprimant la référence au mécanisme de contrôle de la cohérence du paragraphe 1 et en supprimant entièrement le paragraphe 3.

protection des données peuvent être adoptées par le secrétaire d'État (article 17C) ou le commissaire à l'information (article 119A), conformément à la DPA 2018.

(80) En l'absence d'une décision d'adéquation ou de garanties appropriées, un transfert ne peut avoir lieu que sur la base des dérogations énoncées à l'article 49 du RGPD britannique[76]. Le RGPD britannique n'apporte aucune modification de fond aux dérogations par rapport aux règles correspondantes du règlement (UE) 2016/679. En vertu du RGPD britannique comme en vertu du règlement (UE) 2016/679, il n'est possible de recourir à certaines dérogations que si le transfert revêt un caractère occasionnel[77]. En outre, dans ses orientations sur les transferts internationaux, l'ICO précise ce qui suit: «Il convient de ne les appliquer qu'en tant que véritables "exceptions" à la règle générale selon laquelle vous ne devez pas procéder à un transfert restreint, sauf si celui-ci est couvert par une décision d'adéquation ou si des garanties appropriées sont en place»[78]. En ce qui concerne les transferts nécessaires pour des motifs importants d'intérêt public [article 49, paragraphe 1, point d)], le secrétaire d'État peut adopter des règlements afin de préciser les circonstances dans lesquelles un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale n'est pas nécessaire pour des motifs importants d'intérêt public. En outre, le secrétaire d'État peut, par voie de règlements, restreindre le transfert d'une catégorie de données à caractère personnel vers un pays tiers ou à une organisation internationale lorsque celui-ci ne peut avoir lieu sur le fondement de règlements d'adéquation et lorsque le secrétaire d'État considère que cette limitation est nécessaire pour des motifs importants d'intérêt public. Aucun règlement de ce type n'a été adopté à ce jour.

---

76 Conformément à l'article 49 du RGPD britannique, les transferts sont possibles si l'une des conditions suivantes est remplie: a) la personne concernée a donné son consentement explicite au transfert envisagé, après avoir été informée des risques que ce transfert pouvait comporter pour elle en raison de l'absence de décision d'adéquation et de garanties appropriées; b) le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée; c) le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable du traitement et une autre personne physique ou morale; d) le transfert est nécessaire pour des motifs importants d'intérêt public; e) le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice; f) le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement; g) le transfert a lieu au départ d'un registre qui, conformément au droit interne, est destiné à fournir des informations au public et est ouvert à la consultation du public en général ou de toute personne justifiant d'un intérêt légitime, mais uniquement dans la mesure où les conditions prévues pour la consultation dans le droit interne sont remplies dans le cas d'espèce. De plus, si aucune des conditions ci-dessus n'est applicable, un transfert ne peut avoir lieu que s'il ne revêt pas de caractère répétitif, ne touche qu'un nombre limité de personnes concernées, est nécessaire aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement sur lesquels ne prévalent pas les intérêts ou les droits et libertés de la personne concernée, et si le responsable du traitement a évalué toutes les circonstances entourant le transfert de données et a offert, sur la base de cette évaluation, des garanties appropriées en ce qui concerne la protection des données à caractère personnel.

77 Le considérant 111 du RGPD britannique précise que les transferts dans le cadre d'un contrat ou d'une action en justice ne peuvent avoir lieu que s'ils sont occasionnels.

78 Orientations de l'ICO sur les transferts internationaux, disponibles à l'adresse suivante: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/#ib7

(81) Ce cadre relatif aux transferts internationaux est devenu applicable à la fin de la période de transition[79]. Cependant, l'annexe 21, point 4, de la DPA 2018 (introduite par la réglementation DPPEC) prévoit qu'à partir de la fin de la période de transition, certains transferts de données à caractère personnel sont traités comme s'ils étaient fondés sur des règlements d'adéquation. Sont compris les transferts vers un État de l'EEE, le territoire de Gibraltar, une institution, un organe ou un organisme de l'Union créé par le traité UE ou en vertu de celui-ci, et les pays tiers qui faisaient l'objet d'une décision d'adéquation de l'Union à la fin de la période de transition. En conséquence, les transferts vers ces pays peuvent se poursuivre dans les mêmes conditions que celles en vigueur avant le retrait du Royaume-Uni de l'Union européenne. Après la fin de la période de transition, le secrétaire d'État doit procéder à un examen des présentes conclusions sur l'adéquation au cours d'une période de quatre ans, à savoir d'ici la fin du mois de décembre 2024. Selon les explications fournies par les autorités britanniques, bien que le secrétaire d'État doive procéder à cet examen avant fin décembre 2024, les dispositions transitoires n'incluent pas de disposition de «caducité» et les dispositions transitoires pertinentes ne cesseront pas automatiquement de produire leurs effets si l'examen n'est pas terminé d'ici la fin du mois de décembre 2024.

(82) Enfin, en ce qui concerne l'évolution future du régime des transferts internationaux du Royaume-Uni — par l'adoption de nouveaux règlements d'adéquation, la conclusion d'accords internationaux ou l'élaboration d'autres mécanismes de transfert — la Commission suivra de près la situation, évaluera si les différents mécanismes de transfert sont utilisés de manière à garantir la continuité de la protection et, le cas échéant, prendra les mesures appropriées pour remédier aux éventuels effets négatifs de cette continuité (voir considérants (278) à (287)). Étant donné que l'UE et le Royaume-Uni partagent des règles similaires en matière de transferts internationaux, on s'attend à ce que les divergences problématiques soient également évitées par la coopération, l'échange d'informations et le partage d'expériences, y compris entre l'ICO et le comité européen de la protection des données.

2.5.8 Responsabilité

(83) Selon le principe de responsabilité, les entités traitant des données sont tenues de mettre en place les mesures techniques et organisationnelles appropriées pour s'acquitter effectivement de leurs obligations en matière de protection des données et doivent être en mesure de démontrer le respect de ces obligations, en particulier à l'autorité de contrôle compétente.

(84) Le principe de responsabilité établi dans le règlement (UE) 2016/679 a été conservé à l'article 5, paragraphe 2, du RGPD britannique sans modifications de fond. Il en va de même pour l'article 24 relatif à la responsabilité du responsable du traitement, pour l'article 25 relatif à la protection des données dès la conception et par défaut et pour l'article 30 relatif aux registres des activités de traitement. Les articles 35 et 36 relatifs à l'analyse d'impact relative à la protection des données et à la consultation préalable de l'autorité de contrôle ont également été conservés. Les articles 37 à 39 du règlement

[79] Durant une période maximale de six mois se terminant au plus tard le 30 juin 2021, l'applicabilité de ce nouveau cadre doit être interprétée à la lumière de 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 (JO L 444/14 du 31.12.2020) (l'«ACC UE-Royaume-Uni»), disponible à l'adresse suivante: https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:22020A1231(01)&from=FR.

(UE) relatifs à la désignation et aux missions du délégué à la protection des données ont été conservés dans le RGPD britannique sans modifications de fond. Par ailleurs, les dispositions des articles 40 et 42 du règlement (UE) 2016/679 relatives aux codes de conduite et à la certification ont été conservées dans le RGPD britannique[80].

2.6 Surveillance et contrôle de l'application des règles

2.6.1 Surveillance indépendante

(85) Pour garantir un niveau adéquat de protection des données dans la pratique, il convient de mettre en place une autorité de contrôle indépendante chargée de surveiller l'application des règles en matière de protection des données et de les faire respecter. Cette autorité devrait agir en toute indépendance et en toute impartialité dans l'exercice de ses fonctions et compétences.

(86) Au Royaume-Uni, l'autorité chargée de surveiller l'application du RGPD britannique et de la DPA 2018 et de les faire respecter est le commissaire à l'information. Le commissaire à l'information est une «personne morale individuelle»: une entité juridique distincte constituée en une seule personne. Le commissaire à l'information est soutenu dans ses fonctions par un bureau. Le 31 mars 2020, le personnel permanent du Bureau du commissaire à l'information comptait 768 membres[81]. Le ministère parrain du commissaire à l'information est le ministère du numérique, de la culture, des médias et du sport[82].

(87) L'indépendance du commissaire à l'information est expressément établie à l'article 52 du RGPD britannique, lequel n'apporte aucune modification de fond à l'article 52, paragraphes 1 à 3, du RGPD. Conformément au RGPD britannique, le commissaire doit agir en toute indépendance dans l'exercice de ses missions et de ses pouvoirs, demeurer libre de toute influence extérieure, qu'elle soit directe ou indirecte, en lien avec ces missions et ses pouvoirs, et ne solliciter ni n'accepter d'instructions de quiconque. Le commissaire doit également s'abstenir de tout acte incompatible avec ses fonctions et, pendant la durée de son mandat, n'exercer aucune activité professionnelle incompatible, rémunérée ou non.

(88) Les conditions relatives à la nomination et à la révocation du commissaire à l'information sont énoncées à l'annexe 12 de la DPA 2018. Le commissaire à l'information est nommé par Sa Majesté sur recommandation du gouvernement, dans

---

80 Le cas échéant, les références à l'autorité de contrôle compétente sont remplacées par des références aux autorités du Royaume-Uni. Par exemple, en vertu de l'article 17 de la DPA 2018, le commissaire à l'information ou l'organisme national d'accréditation du Royaume-Uni peut agréer une personne satisfaisant aux exigences énoncées à l'article 43 du RGPD britannique pour contrôler le respect d'une certification.

81 Rapport annuel et états financiers du commissaire à l'information pour la période 2019-2020, disponibles à l'adresse suivante: https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf

82 Un accord de gestion régit la relation entre les deux parties. En particulier, les principales responsabilités du DCMS, en qualité de ministère parrain, consistent: à s'assurer que le commissaire à l'information reçoit un financement et des ressources appropriés; à représenter les intérêts du commissaire à l'information auprès du Parlement et des autres ministères; à garantir la mise en place d'un cadre national de protection des données solide; et à fournir des orientations et une assistance au Bureau du commissaire à l'information sur les questions opérationnelles ayant trait, par exemple, à l'immobilier, aux contrats de location et aux marchés publics (accord de gestion 2018-2021, disponible à l'adresse suivante: https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf).

le respect d'une concurrence loyale et ouverte. Le candidat doit justifier des qualifications et des compétences appropriées. Conformément au code de gouvernance pour les nominations publiques[83], un panel d'évaluation consultatif dresse une liste des candidats retenus. Avant que le secrétaire d'État au numérique, à la culture, aux médias et au sport ne rende sa décision finale, la commission spéciale compétente du Parlement doit procéder à un examen préalable minutieux. L'avis de la commission est ensuite rendu public[84].

(89) Le commissaire à l'information exerce ses fonctions pour un mandat d'une durée maximale de sept ans. Une personne ne peut être nommée qu'une seule fois à ce poste. Le commissaire à l'information peut être démis de ses fonctions par Sa Majesté à la suite d'une intervention des deux chambres du Parlement[85]. Une demande de révocation du commissaire à l'information ne peut être présentée devant l'une des deux chambres du Parlement, sauf si un ministre de la Couronne a soumis un rapport indiquant que le commissaire à l'information a commis une faute grave et/ou qu'il ne remplit plus les conditions requises pour exercer les fonctions de commissaire[86].

(90) Le financement du commissaire à l'information provient de trois sources: i) les redevances pour la protection des données payées par les responsables du traitement, qui sont fixées par la réglementation du secrétaire d'État[87] [réglementation de 2018 sur la protection des données (redevances et informations)] et qui représentent entre 85 % et 90 % du budget annuel du bureau[88]; ii) la subvention versée par le gouvernement au commissaire à l'information. Cette subvention sert principalement à financer les frais de fonctionnement du commissaire à l'information en ce qui concerne ses missions non liées à la protection des données[89]; et iii) les frais facturés pour la prestation de services[90]. À l'heure actuelle, de tels frais n'ont pas été facturés.

---

83 Code de gouvernance pour les nominations publiques, disponible à l'adresse suivante: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/578498/governance_code_on_public_appointments_16_12_2016.pdf

84 Deuxième rapport de la session 2015-2016 de la commission de la culture, des médias et du sport de la Chambre des communes, disponible à l'adresse suivante: https://publications.parliament.uk/pa/cm201516/cmselect/cmcumeds/990/990.pdf

85 Une «intervention» est une motion déposée devant le Parlement qui vise à informer le monarque des avis du Parlement sur une question spécifique.

86 Annexe 12, point 3, sous 3), de la DPA 2018.

87 Article 137 de la DPA 2018, voir le considérant (17).

88 Les articles 137 et 138 de la DPA 2018 contiennent un certain nombre de garanties afin de faire en sorte que le montant des redevances soit fixé à un niveau approprié. En particulier, l'article 137, paragraphe 4, énumère les éléments que le secrétaire d'État doit prendre en considération au moment d'adopter les règlements qui précisent le montant que doivent verser différentes organisations; deuxièmement, l'article 138, paragraphe 1, et l'article 182 de la DPA 2018 soumettent le secrétaire d'État à l'obligation juridique de consulter, avant l'adoption des règlements, le commissaire à l'information et d'autres représentants de personnes susceptibles d'être concernées par lesdits règlements afin que leurs points de vue soient pris en compte. En outre, en vertu de l'article 138, paragraphe 2, de la DPA 2018, le commissaire à l'information est tenu d'examiner régulièrement le fonctionnement des règlements relatifs aux redevances et peut soumettre au secrétaire d'État des propositions de modification de ces derniers. Enfin, à moins qu'ils ne soient adoptés simplement pour prendre en compte une hausse de l'indice des prix de détail (auquel cas ils seront soumis à la procédure de résolution négative), les règlements sont soumis à la procédure de résolution positive et ne peuvent être adoptés avant d'avoir été approuvés par résolution de chaque chambre du Parlement.

89 L'accord de gestion précise que «le secrétaire d'État peut effectuer des paiements en faveur du commissaire à l'information à partir des fonds versés par le Parlement au titre de l'annexe 12, point 9, de la DPA 2018. Après consultation du commissaire à l'information, le DCMS versera à ce dernier les

(91) Les fonctions générales du commissaire à l'information relatives au traitement de données à caractère personnel auquel s'applique le RGPD britannique sont définies à son article 57 et reflètent étroitement les règles correspondantes du règlement (UE) 2016/679. Ses fonctions consistent entre autres à contrôler l'application du RGPD britannique et à veiller au respect de celui-ci, à favoriser la sensibilisation du public, à traiter les réclamations introduites par les personnes concernées, à effectuer des enquêtes, etc. En outre, l'article 115 de la DPA 2018 décrit d'autres fonctions générales du commissaire, parmi lesquelles figurent le devoir de conseiller le Parlement, le gouvernement et d'autres institutions et organes sur les mesures législatives et administratives relatives à la protection des droits et libertés des personnes à l'égard du traitement des données à caractère personnel les concernant, et le pouvoir d'émettre, de sa propre initiative ou sur demande, des avis à l'attention du Parlement, du gouvernement ou d'autres institutions et organismes ainsi que du public, sur toute question relative à la protection des données à caractère personnel. Afin de préserver l'indépendance du pouvoir judiciaire, le commissaire à l'information n'est pas autorisé à exercer ses fonctions dans le cadre du traitement de données à caractère personnel par une personne ou une juridiction agissant dans l'exercice de la fonction juridictionnelle. Toutefois, la surveillance du pouvoir judiciaire est assurée par des organes spécialisés [voir les considérants (99) à (103)].

2.6.2 Contrôle de l'application des règles, y compris les sanctions

(92) Les pouvoirs du commissaire à l'information sont décrits à l'article 58 du RGPD britannique, qui n'apporte aucune modification de fond à l'article correspondant du règlement (UE) 2016/679. La DPA 2018 fixe des règles complémentaires concernant les modalités d'exercice de ces pouvoirs. Le commissaire dispose notamment des pouvoirs suivants: a) ordonner au responsable du traitement et au sous-traitant (et dans certains cas à toute autre personne) de lui communiquer les informations nécessaires en délivrant un avis d'information (ci-après «avis d'information»)[91]; b) mener des enquêtes et réaliser des audits en émettant un avis d'évaluation, qui peut obliger le responsable du traitement ou le sous-traitant à autoriser le commissaire à pénétrer dans des locaux spécifiques, à inspecter ou à examiner des documents ou des équipements, à interroger les personnes chargées du traitement des données à caractère personnel pour le compte du responsable du traitement, etc. (ci-après «avis d'évaluation»)[92]; c) obtenir de toute autre manière l'accès aux documents, etc., des responsables du traitement et des sous-traitants, ainsi que l'accès à leurs locaux, conformément à l'article 154 de la DPA 2018 («pouvoirs d'accès et d'inspection»); d) exercer le pouvoir d'adopter des mesures correctrices, notamment au moyen d'avertissements et de rappels à l'ordre, ou ordonner au responsable du traitement/sous-traitant, par voie d'avis d'exécution, de prendre ou de s'abstenir de prendre des mesures spécifiques, notamment lui ordonner d'accomplir toute action visée à l'article 58, paragraphe 2), points c) à g) et j), du RGPD britannique (ci-après «avis d'exécution»)[93]; e) et infliger des amendes administratives sous la forme d'un avis de sanction (ci-après «avis de

---

montants correspondants (la subvention) pour les frais administratifs de l'ICO et l'exercice de ses fonctions ayant trait à un certain nombre de missions spécifiques, notamment la liberté de l'information» (accord de gestion 2018-2021, point 1.12, voir la note de bas de page 82).

90 Voir l'article 134 de la DPA 2018.

91 Article 142 de la DPA 2018 (sous réserve des limitations prévues à son article 143).

92 Article 146 de la DPA 2018 (sous réserve des limitations prévues à son article 147).

93 Articles 149 à 151 de la DPA 2018 (sous réserve des limitations prévues à son article 152).

sanction»)[94]. Ce dernier peut également être délivré dans le cas où une autorité publique n'a pas respecté les dispositions du RGPD britannique[95].

(93) La politique d'action réglementaire de l'ICO décrit les circonstances dans lesquelles il émettra un avis d'information, d'évaluation, d'exécution ou de sanction[96]. Un avis d'exécution délivré à la suite d'un manquement d'un responsable du traitement ou d'un sous-traitant peut uniquement imposer les exigences que le commissaire juge appropriées afin de remédier au manquement. Des avis d'exécution et de sanction peuvent être délivrés à un responsable du traitement ou à un sous-traitant dans le cas des violations visées au chapitre II (principes relatifs au traitement), aux articles 12 à 22 (droits de la personne concernée), aux articles 25 à 39 (obligations qui incombent aux responsables du traitement et aux sous-traitants) et aux articles 44 à 49 (transferts internationaux) du RGPD britannique. Un avis d'exécution peut également être délivré à un responsable du traitement qui n'a pas respecté l'obligation de payer la redevance fixée par les règlements adoptés en vertu de l'article 137 de la DPA 2018. En outre, un organisme chargé du suivi au titre de l'article 41 ou un prestataire de services de certification peut se voir délivrer un avis d'exécution s'il n'a pas respecté les obligations découlant du RGPD britannique. Un avis de sanction peut également être délivré à une personne qui ne s'est pas conformée à un avis d'information, à un avis d'évaluation ou à un avis d'exécution.

(94) L'avis de sanction oblige la personne à s'acquitter auprès du commissaire à l'information du montant indiqué dans l'avis. Pour décider s'il y a lieu de délivrer un avis de sanction à une personne et pour déterminer le montant de la sanction, le commissaire à l'information doit tenir compte des éléments énumérés à l'article 83, paragraphes 1 et 2, du RGPD britannique, lesquels sont identiques aux règles correspondantes du règlement (UE) 2016/679[97]. Conformément à l'article 83, paragraphes 4 et 5, le montant maximal des amendes administratives en cas de manquement aux obligations visées dans ces dispositions est respectivement de 8 700 000 GBP ou de 17 500 000 GBP. Dans le cas d'une entreprise, le commissaire à l'information peut également infliger des amendes correspondant à un pourcentage du chiffre d'affaires annuel mondial, si le montant est plus élevé. Comme dans les dispositions équivalentes du règlement (UE) 2016/679, ces montants sont fixés respectivement à 2 % et 4 % dans l'article 83, paragraphes 4 et 5. En cas de non-

94 Article 155 de la DPA 2018 et article 83 du RGPD britannique.

95 C'est ce qui ressort de l'article 155, point 1, de la DPA de 2018, lue conjointement avec l'article 149, points 2 et 5, de la DPA de 2018, et de l'article 156, point 4, de la DPA de 2018, qui limite la délivrance d'avis de sanctions uniquement à l'égard des commissaires du patrimoine de la Couronne et des contrôleurs pour la Maison royale conformément à l'article 209, point 4, de la DPA 2018.

96 Politique d'action réglementaire, disponible à l'adresse suivante: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf

97 Y compris la nature et la gravité de la violation (compte tenu de la nature, de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et du niveau de dommage qu'elles ont subi), le fait que la violation a été commise délibérément ou par négligence, toute mesure prise par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées, le degré de responsabilité du responsable du traitement ou du sous-traitant (compte tenu des mesures techniques et organisationnelles qu'ils ont mises en œuvre), toute violation pertinente commise précédemment par le responsable du traitement ou le sous-traitant; le degré de coopération établi avec le commissaire, les catégories de données à caractère personnel concernées par le manquement, toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce, telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation.

respect d'un avis d'information, d'un avis d'évaluation ou d'un avis d'exécution, le montant maximal de la sanction qui peut être imposée par voie d'avis de sanction s'élève à 17 500 000 GBP ou, dans le cas d'une entreprise, à 4 % du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

(95) Le RGPD britannique, de même que la DPA 2018, a également renforcé d'autres pouvoirs du commissaire à l'information. Par exemple, le commissaire peut désormais procéder à des audits obligatoires auprès de l'ensemble des responsables du traitement et des sous-traitants au moyen des avis d'évaluation, tandis que, en vertu de la législation précédente, la loi de 1998 sur la protection des données, il ne disposait de ce pouvoir qu'à l'égard des autorités centrales et des organisations de santé, les autres entités et personnes devant accepter de se soumettre à un audit.

(96) Depuis l'introduction du règlement (UE) 2016/679, l'ICO traite environ 40 000 réclamations de personnes concernées par an[98] et, en outre, mène environ 2 000 enquêtes d'office[99]. La majorité des réclamations sont liées aux droits d'accès aux données et à la communication des données. À l'issue de ses enquêtes, le commissaire prend des mesures répressives dans un large éventail de secteurs. Plus précisément, selon le dernier rapport annuel (2019-2020) du commissaire à l'information[100], le commissaire a émis 54 avis d'information, 8 avis d'évaluation, 7 avis d'exécution et 4 avertissements, a entamé 8 poursuites et a infligé 15 amendes au cours de la période de référence[101].

(97) Ces mesures comprennent plusieurs sanctions pécuniaires importantes imposées en vertu du règlement (UE) 2016/679 et de la DPA 2018. Le commissaire à l'information a notamment infligé, en octobre 2020, une amende de 20 millions de livres sterling à une compagnie aérienne britannique pour une violation de données concernant plus de 400 000 clients. À la fin du mois d'octobre 2020, une chaîne d'hôtel internationale

98 Selon les informations fournies par les autorités britanniques, au cours de la période couverte par le rapport annuel 2019-2020 du commissaire à l'information, aucune violation n'a été constatée dans environ 25 % des cas; dans environ 29 % des cas, la personne concernée a été invitée à signaler le problème en premier lieu au responsable du traitement, à attendre sa réponse ou à maintenir le dialogue avec celui-ci; dans environ 17 % des cas, aucune violation n'a été constatée, mais le responsable du traitement a reçu des conseils; dans environ 25 % des cas, le commissaire à l'information a constaté une violation et a dispensé des conseils au responsable du traitement ou ce dernier a été contraint de prendre certaines mesures; dans environ 3 % des cas, il a été établi que la réclamation ne relevait pas du règlement (UE) 2016/679; et environ 1 % des cas ont été renvoyés devant une autre autorité de protection des données dans le cadre du comité européen de la protection des données.

99 L'ICO peut ouvrir ces enquêtes sur la base d'informations reçues de diverses sources, notamment de notifications de violation de données à caractère personnel, de renvois par d'autres autorités publiques du Royaume-Uni ou des autorités étrangères de protection des données, et de réclamations émanant de particuliers ou d'organisations de la société civile.

100 Rapport annuel et états financiers du commissaire à l'information pour la période 2019-2020 (voir la note de bas de page 81).

101 Selon son précédent rapport annuel couvrant la période 2018-2019, le commissaire à l'information a émis, au cours de la période considérée, 22 avis de sanction au titre de la DPA 1998 et a infligé des amendes pour un montant total de 3 010 610 GBP, dont deux amendes s'élevant à 500 000 GBP (le montant maximal autorisé par la DPA 1998). En 2018, le commissaire à l'information a notamment enquêté sur l'utilisation des données analytiques à des fins politiques à la suite des révélations liées à Cambridge Analytica. L'enquête a donné lieu à un rapport de police, à une série de recommandations, à une amende de 500 000 GBP à l'encontre de Facebook et à un avis d'application adressé à Aggregate IQ, un courtier de données canadien, ordonnant à la société de supprimer les données à caractère personnel qu'elle détenait concernant les citoyens et résidents du Royaume-Uni (voir le rapport annuel et les états financiers du commissaire à l'information pour la période 2018-2019, disponibles à l'adresse suivante: https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf).

s'est vu infliger une amende de 18,4 millions de livres sterling pour n'avoir pas veillé à la protection des données à caractère personnel de millions de clients et, en novembre 2020, un fournisseur de services britannique vendant des billets pour des manifestations en ligne a été condamné à verser une amende de 1,25 million de livres sterling pour n'avoir pas protégé les coordonnées bancaires de ses clients[102].

(98) Outre les pouvoirs d'application des règles du commissaire à l'information décrits au considérant (92), certaines violations de la législation en matière de protection des données constituent des infractions et peuvent par conséquent faire l'objet de sanctions pénales (article 196 de la DPA 2018). Ces infractions consistent, par exemple, à obtenir ou à divulguer sciemment ou imprudemment des données à caractère personnel sans le consentement du responsable du traitement, à obtenir la divulgation de données à caractère personnel à une autre personne sans le consentement du responsable du traitement[103], à réidentifier des informations qui constituent des données à caractère personnel anonymisées sans le consentement du responsable du traitement responsable de l'anonymisation de ces données[104], à empêcher, de manière intentionnelle, le commissaire d'exercer ses pouvoirs dans le cadre de l'inspection de données à caractère personnel conformément aux obligations internationales[105], à faire de fausses déclarations en réponse à un avis d'information, ou à détruire des informations en rapport avec des avis d'information et d'évaluation[106].

2.6.3 Surveillance du pouvoir judiciaire

(99) La surveillance du traitement des données à caractère personnel par les juridictions et les juges comporte deux dimensions. Lorsque le titulaire d'une fonction de juge ou une juridiction n'agit pas dans l'exercice de sa fonction juridictionnelle, la surveillance est assurée par l'ICO. Lorsque le responsable du traitement agit dans l'exercice de sa fonction juridictionnelle, l'ICO ne peut exercer ses fonctions de surveillance[107] et la surveillance est assurée par des organismes spéciaux. Cette approche correspond à celle adoptée dans le règlement (UE) 2016/679 (article 55, paragraphe 3).

(100) En particulier, dans le deuxième scénario, dans le cas des juridictions d'Angleterre et du pays de Galles et des tribunaux de première instance et supérieurs d'Angleterre et du pays de Galles, cette surveillance est assurée par le panel de protection des données judiciaires[108]. En outre, le président de la Haute Cour et le Premier Président des

---

102 Pour une synthèse des mesures répressives prises, voir le site internet de l'ICO à l'adresse suivante: https://ico.org.uk/action-weve-taken/enforcement/

103 Article 170 de la DPA 2018.

104 Article 171 de la DPA 2018.

105 Article 119 de la DPA 2018.

106 Articles 144 et 148 de la DPA 2018.

107 Article 117 de la DPA 2018.

108 Le panel est chargé de fournir des orientations et de dispenser des formations aux juges. Il traite également les réclamations des personnes concernées relatives au traitement des données à caractère personnel les concernant par les juridictions et les personnes agissant dans l'exercice de leur fonction juridictionnelle. Le panel vise à fournir les outils permettant de régler toute réclamation. Si l'auteur d'une réclamation n'est pas satisfait d'une décision du panel et qu'il apporte de nouvelles preuves, le panel peut revenir sur sa décision. Bien qu'il n'impose pas lui-même de sanctions financières, si le panel considère qu'il existe une violation suffisamment grave de la DPA 2018, il peut saisir le Bureau des enquêtes en matière de conduite judiciaire (JCIO) qui enquêtera sur la réclamation. Si la réclamation est jugée recevable, il appartient au Lord Chancelier et au président de la Haute Cour (ou à un haut magistrat mandaté pour agir en son nom) de décider de la mesure qu'il convient de prendre à l'encontre du titulaire d'une fonction de juge. Il peut s'agir, par ordre de sévérité, des mesures suivantes: un avis

tribunaux ont publié une déclaration de protection des données[109] qui définit les modalités de traitement des données à caractère personnel par les juridictions d'Angleterre et du pays de Galles dans le cadre de leur fonction juridictionnelle. Une déclaration similaire a été publiée par les autorités judiciaires d'Irlande du Nord[110] et d'Écosse[111].

(101) De plus, en Irlande du Nord, le président de la Haute Cour a nommé un juge de la Haute Cour en qualité de juge chargé de la surveillance des données[112]. Il a également publié des orientations à l'intention des juges d'Irlande du Nord sur les mesures à prendre en cas de perte potentielle ou avérée de données et sur les modalités de gestion des problèmes qui en découlent[113].

(102) En Écosse, le *Lord President* (plus haut magistrat) a nommé un juge chargé de la surveillance des données pour enquêter sur toute réclamation fondée sur la protection des données. Ses fonctions sont décrites dans les règles relatives aux plaintes judiciaires qui correspondent à celles établies pour l'Angleterre et le pays de Galles[114].

(103) Pour finir, à la Cour suprême, l'un des juges de la Cour suprême est nommé pour surveiller la protection des données.

2.6.4 Recours

---

formel, un avertissement formel, un rappel à l'ordre et, en dernier lieu, une révocation. Si un particulier n'est pas satisfait de la façon dont le JCIO a enquêté sur sa réclamation, il peut déposer une autre réclamation devant le médiateur des nominations judiciaires et de la déontologie de la magistrature (https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman). Le médiateur a le pouvoir de demander au JCIO d'enquêter de nouveau sur une réclamation et peut proposer l'indemnisation de l'auteur d'une réclamation lorsqu'il considère que ce dernier a subi un préjudice du fait d'une mauvaise gestion.

109 La déclaration de protection des données du président de la Haute Cour et du Premier Président des tribunaux est disponible à l'adresse suivante: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice

110 La déclaration de protection des données publiée par le président de la Haute Cour d'Irlande du Nord est disponible à l'adresse suivante: https://judiciaryni.uk/data-privacy.

111 La déclaration de protection des données pour les juridictions écossaises est disponible à l'adresse suivante: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice

112 Le juge chargé de la surveillance des données fournit des orientations aux juges et enquête sur les violations et/ou les réclamations relatives au traitement de données à caractère personnel par les juridictions ou les personnes agissant dans l'exercice de leur fonction juridictionnelle.

113 Lorsque la réclamation ou la violation est considérée comme grave, celle-ci est soumise au responsable des plaintes judiciaires afin de faire l'objet d'une enquête plus poussée, conformément au code de bonnes pratiques relatif aux plaintes du président de la Haute Cour d'Irlande du Nord. L'issue de la réclamation peut notamment être: aucune suite, des conseils, une formation ou un mentorat, un avertissement informel, un avertissement formel, un avertissement définitif, une pratique restreinte ou un renvoi devant un tribunal prévu par la loi. Le code de bonnes pratiques relatif aux plaintes publié par le président de la Haute Cour d'Irlande du Nord est disponible à l'adresse suivante:https://judiciaryni.uk/sites/judiciary/files/media-files/14G.%20CODE%20OF%20PRACTICE%20Judicial%20~%2028%20Feb%2013%20%28Final%29%20updated%20with%20new%20comp.._1.pdf.

114 Toute réclamation qui s'avère fondée est examinée par le juge chargé de la surveillance des données et est soumise au plus haut magistrat qui a le pouvoir d'émettre un avis, un avertissement formel ou un rappel à l'ordre s'il le juge nécessaire (des règles équivalentes existent pour les membres des tribunaux et sont disponibles à l'adresse suivante: https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2)

(104) En vue d'une protection adéquate et, en particulier, du respect de ses droits individuels, la personne concernée doit disposer de possibilités de recours administratif et juridictionnel effectif, y compris d'indemnisation.

(105) Premièrement, une personne concernée a le droit d'introduire une réclamation auprès du commissaire à l'information si elle considère qu'une violation du RGPD britannique a été commise en lien avec des données à caractère personnel la concernant[115]. Le RGPD britannique conserve les règles prévues par l'article 77 du règlement (UE) 2016/679 relatives à ce droit, sans modifications de fond. Il en va de même pour les dispositions de l'article 57, paragraphe 1, point f), et de l'article 57, et paragraphe 2, qui décrivent les missions du commissaire dans le cadre du traitement des réclamations. Comme décrit aux considérants (92) à (98) above, le commissaire à l'information a le pouvoir d'évaluer le respect du RGPD britannique et de la DPA 2018 par le responsable du traitement et le sous-traitant, de les obliger à prendre ou à s'abstenir de prendre les mesures nécessaires en cas de non-respect et d'infliger des amendes.

(106) Deuxièmement, le RGPD britannique et la DPA 2018 prévoient le droit à un recours contre le commissaire à l'information. Conformément à l'article 78, paragraphe 1, du RGPD britannique, toute personne concernée a le droit de former un recours juridictionnel effectif contre une décision juridiquement contraignante du commissaire qui la concerne. Dans le cadre du contrôle juridictionnel, le juge examine la décision contestée dans la réclamation et détermine si le commissaire à l'information a agi légalement ou non. En outre, conformément à l'article 78, paragraphe 2, du RGPD britannique, si le commissaire ne traite pas une réclamation introduite par la personne concernée de manière appropriée,[116] l'auteur de la réclamation a le droit de former un recours juridictionnel. Il peut demander au tribunal de première instance d'ordonner au commissaire de prendre les mesures appropriées pour donner suite à la réclamation ou de tenir l'auteur de la réclamation informé de son état d'avancement[117]. En outre, toute personne qui reçoit l'un des avis susmentionnés (avis d'information, d'évaluation, d'exécution ou de sanction) délivré par le commissaire peut former un recours devant le tribunal de première instance[118]. S'il considère que la décision du commissaire n'est pas conforme au droit ou que le commissaire à l'information aurait dû exercer son pouvoir discrétionnaire différemment, le tribunal doit faire droit au recours ou remplacer la décision du commissaire par un autre avis ou une autre décision que celui-ci aurait pu émettre ou prendre.

(107) Troisièmement, les personnes concernées peuvent former un recours juridictionnel contre les responsables du traitement et les sous-traitants directement devant les tribunaux en vertu de l'article 79 du RGPD britannique et de l'article 167 de la DPA 2018. Si, dans le cas d'une demande introduite par une personne concernée, une juridiction constate une violation des droits qui sont conférés à la personne concernée

---

115 Article 77 du RGPD britannique.

116 L'article 166 de la DPA 2018 mentionne spécifiquement les situations suivantes: a) le commissaire ne prend pas les mesures appropriées pour donner suite à la réclamation, b) le commissaire n'informe pas l'auteur de la réclamation de l'état d'avancement ou de l'issue de la réclamation avant l'expiration du délai de trois mois à compter de la date de réception de la réclamation par le commissaire, ou c) si l'examen de la réclamation par le commissaire n'est pas mené à terme dans ce délai, le commissaire n'en informe pas l'auteur de la réclamation dans un nouveau délai de trois mois.

117 Article 78, paragraphe 2, du RGPD britannique et article 166 de la DPA 2018.

118 Article 78, paragraphe 1, du RGPD britannique et article 162 de la DPA 2018.

par la législation en matière de protection des données, elle peut ordonner au responsable du traitement, en ce qui concerne le traitement, ou au sous-traitant agissant pour le compte de celui-ci, de prendre ou de s'abstenir de prendre les mesures indiquées dans la décision.

(108) De plus, en vertu de l'article 82 du RGPD britannique et de l'article 168 de la DPA 2018, toute personne ayant subi un dommage matériel ou moral du fait d'une violation du RGPD britannique a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi. Les règles en matière de réparation et de responsabilité énoncées à l'article 82, paragraphes 1 à 5, du RGPD britannique sont identiques aux règles correspondantes du règlement (UE) 2016/679. En vertu de l'article 168 de la DPA 2018, un préjudice moral inclut également une souffrance. En vertu de l'article 80 du RGPD britannique, la personne concernée a également le droit de mandater un organisme ou une organisation de représentation pour qu'il introduise une réclamation en son nom auprès du commissaire (au titre de l'article 77 du RGPD britannique) et exerce en son nom les droits visés aux articles 78 (droit à un recours juridictionnel effectif contre le commissaire), 79 (droit à un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant) et 82 (droit à réparation et responsabilité) du RGPD britannique.

(109) Quatrièmement, en sus des différentes possibilités de recours décrites ci-dessus, toute personne qui considère que ses droits, y compris ses droits au respect de la vie privée et à la protection des données, ont été violés par une autorité publique peut demander réparation auprès des juridictions du Royaume-Uni au titre de la loi de 1998 sur les droits de l'homme[119]. Une personne prétendant qu'une autorité publique a agi (ou propose d'agir) d'une manière qui est incompatible avec un droit reconnu par la convention et, par conséquent, illégale au sens de l'article 6, paragraphe 1, de la loi de 1998 sur les droits de l'homme, peut intenter une action contre cette autorité auprès de la juridiction compétente ou exercer les droits concernés dans toute procédure judiciaire, lorsqu'elle est (ou se prétend) victime d'un acte illégal.

(110) Si la juridiction constate le caractère illégal d'un acte de l'autorité publique, elle peut, dans la limite de ses pouvoirs, prendre toute mesure ou toute ordonnance qu'elle considère comme juste et appropriée[120]. La juridiction peut également déclarer une disposition de droit primaire incompatible avec un droit reconnu par la convention.

(111) Enfin, après avoir épuisé les voies de recours internes, une personne physique peut obtenir réparation auprès de la Cour européenne des droits de l'homme en cas de violation des droits garantis par la convention européenne des droits de l'homme.

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

(112) La Commission a également évalué le cadre juridique du Royaume-Uni en ce qui concerne la collecte et l'utilisation ultérieure des données à caractère personnel transférées à des opérateurs économiques au Royaume-Uni par les autorités publiques

119 Article 7, paragraphe 1, de la loi de 1998 sur les droits de l'homme. Conformément à l'article 7, paragraphe 7, une personne n'est victime d'un acte illégal que si elle se prétend victime au regard de l'article 34 de la convention européenne des droits de l'homme dans le cadre d'une procédure engagée devant la Cour européenne des droits de l'homme concernant cet acte.

120 Article 8, paragraphe 1, de la loi de 1998 sur les droits de l'homme.

britanniques pour des motifs d'intérêt public, en particulier à des fins répressives et à des fins de sécurité nationale (ci-après l'«accès des pouvoirs publics»). Lorsqu'elle a évalué si les conditions dans lesquelles les pouvoirs publics accèdent aux données transférées vers le Royaume-Uni en vertu de la présente décision remplissaient le critère de l'«équivalence essentielle» conformément à l'article 45, paragraphe 1, du règlement (UE) 2016/679, tel qu'il est interprété par la Cour de justice de l'Union européenne à la lumière de la Charte des droits fondamentaux, la Commission a notamment pris en compte les critères suivants.

(113) En premier lieu, toute limitation du droit à la protection des données à caractère personnel doit être prévue par la loi et la base juridique qui permet l'ingérence dans ce droit doit définir elle-même la portée de la limitation de l'exercice du droit concerné[121].

(114) En second lieu, pour satisfaire à l'exigence de proportionnalité selon laquelle les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire dans une société démocratique pour répondre à des objectifs spécifiques d'intérêt général équivalents à ceux reconnus par l'Union, la réglementation du pays tiers en cause permettant l'ingérence doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données ont été transférées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus[122]. Elle doit en particulier indiquer en quelles circonstances et sous quelles conditions une mesure prévoyant le traitement de telles données peut être prise[123], ainsi que soumettre le respect de ces exigences à une surveillance indépendante[124].

(115) En troisième lieu, cette législation doit être juridiquement contraignante en vertu du droit interne et ces exigences légales doivent revêtir un caractère non seulement contraignant pour les autorités, mais également opposable devant les juridictions contre les autorités du pays tiers en cause[125]. En particulier, les personnes concernées doivent disposer de la possibilité d'exercer des voies de droit devant un tribunal indépendant et impartial afin d'avoir accès à des données à caractère personnel les concernant, ou d'obtenir la rectification ou la suppression de telles données[126].

---

121 Voir l'arrêt Schrems II, points 174 et 175, et la jurisprudence citée. Voir également, en ce qui concerne l'accès aux données par les autorités publiques des États membres, l'arrêt dans l'affaire C-623/17, Privacy International, ECLI:EU:C:2020:790, point 65; et les affaires jointes C-511/18, C-512/18 et C-520/18, La Quadrature du Net e.a., EU:C:2020:791, point 175.

122 Voir l'arrêt Schrems II, points 176 et 181, ainsi que la jurisprudence citée. Voir également, en ce qui concerne l'accès aux données par les autorités publiques des États membres, l'arrêt Privacy International, point 68; et l'arrêt La Quadrature du Net e.a., point 132.

123 Voir l'arrêt Schrems II, point 176. Voir également, en ce qui concerne l'accès aux données par les autorités publiques des États membres, l'arrêt Privacy International, point 68; et l'arrêt La Quadrature du Net e.a., point 132.

124 Voir l'arrêt Schrems II, point 179.

125 Voir l'arrêt Schrems II, points 181 et 182.

126 Voir les arrêts Schrems I, point 95, et Schrems II, point 194. À cet égard, la CJUE a notamment souligné que le respect de l'article 47 de la charte des droits fondamentaux, qui garantit le droit à un recours effectif devant un tribunal indépendant et impartial, «participe également du niveau de protection requis au sein de l'Union [et] dont la Commission doit constater le respect avant que celle-ci adopte une décision d'adéquation au titre de l'article 45, paragraphe 1, du RGPD» (arrêt Schrems II, point 186).

3.1 Cadre juridique général

(116) En tant qu'exercice de l'autorité publique, l'accès des pouvoirs publics aux données au Royaume-Uni doit intervenir dans le respect total de la loi. Le Royaume-Uni a ratifié la convention européenne des droits de l'homme [voir le considérant (9) ci-dessus] et toutes les autorités publiques du Royaume-Uni sont tenues d'agir en conformité avec la convention[127]. L'article 8 de la convention exige que toute ingérence dans le droit au respect de la vie privée soit prévue par la loi, soit nécessaire à l'une des finalités visées à l'article 8, paragraphe 2, et soit proportionnée par rapport à cette finalité. L'article 8 exige également que l'ingérence soit «prévisible», c'est-à-dire que sa base juridique soit claire et précise et que la législation contienne les garanties nécessaires pour prévenir les abus.

(117) En outre, dans sa jurisprudence, la Cour européenne des droits de l'homme a précisé que toute ingérence dans le droit au respect de la vie privée et à la protection des données devrait être soumise à un système de contrôle effectif, indépendant et impartial, prévu par un juge ou par un autre organe indépendant[128] (par exemple, une autorité administrative ou un organe parlementaire).

(118) Par ailleurs, les personnes physiques doivent bénéficier d'un recours effectif et la Cour européenne des droits de l'homme a expliqué que ce recours devait être offert par un organe indépendant et impartial qui a édicté son propre règlement de procédure, dont les membres doivent exercer ou avoir exercé de hautes fonctions judiciaires ou être des juristes chevronnés, et qu'il ne doit exister aucun obstacle probatoire à surmonter pour pouvoir saisir cette juridiction. Lors de leur examen des réclamations introduites par des particuliers, l'organe indépendant et impartial devrait avoir accès à tous les documents pertinents, y compris à des informations confidentielles. Enfin, il devrait avoir le pouvoir de remédier à la non-conformité[129].

(119) Le Royaume-Uni a également ratifié la convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (convention 108) et a signé, en 2018, le protocole d'amendement à la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (appelé convention 108+)[130]. Conformément à l'article 9 de la convention 108, il n'est possible de déroger aux principes généraux relatifs à la protection des données (article 5 – Qualité des données), aux règles régissant les catégories particulières de données (article 6 – Catégories particulières de données) et aux droits des personnes concernées (article 8 – Garanties complémentaires pour la personne concernée) que lorsqu'une telle dérogation, prévue par la loi de la Partie, constitue une mesure nécessaire dans une société démocratique à la protection de la sécurité de l'État, à la sûreté publique, aux intérêts monétaires de

127 Article 6 de la loi de 1998 sur les droits de l'homme.

128 Cour européenne des droits de l'homme, Klass et autres c. Allemagne, requête nº 5029/71, points 17 à 51.

129 Cour européenne des droits de l'homme, Kennedy c. Royaume-Uni, requête nº 26839/05, (ci-après l'«arrêt Kennedy»), points 167 et 190.

130 Pour de plus amples informations sur la convention européenne des droits de l'homme et son intégration dans le droit britannique par la loi de 1998 sur les droits de l'homme, ainsi que sur la convention 108, voir le considérant (9) ci-dessus.

l'État ou à la répression des infractions pénales, ou à la protection de la personne concernée et des droits et libertés d'autrui[131].

(120) Par conséquent, du fait de son appartenance au Conseil de l'Europe, de son adhésion à la convention européenne des droits de l'homme et de sa soumission à la compétence de la Cour européenne des droits l'homme, le Royaume-Uni est soumis à un certain nombre d'obligations, consacrées par le droit international, qui encadrent le système d'accès aux données de ses pouvoirs publics sur la base de principes, de garanties et de droits individuels semblables à ceux garantis par le droit de l'Union et applicables aux États membres. Comme souligné au considérant (19), le respect permanent de ces instruments constitue donc un élément particulièrement important de l'évaluation sur laquelle est fondée la présente décision.

(121) En outre, la DPA 2018 prévoit des garanties et des droits spécifiques en matière de protection des données dans le cadre du traitement des données par les autorités publiques, notamment les autorités répressives et les agences de sécurité nationale.

(122) En particulier, le régime applicable au traitement des données à caractère personnel à des fins répressives est décrit à la partie 3 de la DPA 2018, qui a été adoptée afin de transposer la directive (UE) 2016/680. La partie 3 de la DPA 2018 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[132].

(123) La notion d'«autorité compétente» est définie à l'article 30 de la DPA comme une personne figurant sur la liste établie à l'annexe 7 de la DPA 2018, ainsi que comme toute autre personne, dans la mesure où elle exerce des fonctions statutaires pour l'une des fins répressives[133]. Comme expliqué ci-dessous (voir le considérant (139)), certaines autorités compétentes (par exemple l'Agence nationale de lutte contre la criminalité) peuvent faire usage, dans certaines conditions, des pouvoirs conférés par la loi de 2016 sur les pouvoirs d'enquête (IPA 2016). Dans ce cas, les garanties prévues par l'IPA 2016 s'appliqueront en plus de celles prévues par la partie 3 de la DPA 2018. Les services de renseignement [le service secret de renseignement (Secret Intelligence Service), le service de sécurité (Security Service) et le quartier général des

---

131 De la même façon, conformément à l'article 11 de la convention 108+, les limitations applicables à certains droits et obligations découlant de la convention à des fins de sécurité nationale ou de prévention, d'investigation et de répression des infractions pénales et d'exécution des sanctions pénales ne sont autorisées que lorsque ces limitations sont prévues par la loi, respectent l'essence des libertés et droits fondamentaux et constituent une mesure nécessaire et proportionnée dans une société démocratique. Les activités de traitement à des fins de sécurité nationale et de défense doivent également faire l'objet d'un contrôle et d'une supervision indépendants effectifs selon la législation nationale de chaque partie à la convention.

132 Article 31 de la DPA 2018.

133 Les autorités compétentes énumérées à l'annexe 7 n'incluent pas que les forces de police, mais également tous les départements ministériels du gouvernement du Royaume-Uni ainsi que d'autres autorités exerçant des fonctions d'enquête [par exemple le commissaire chargé des recettes et des douanes (Commissioner for Her Majesty's Revenue and Customs), l'Autorité fiscale galloise (Welsh Revenue Authority), l'Autorité de la concurrence et des marchés (Competition and Markets Authority) ou le Cadastre (Her Majesty's Land Register)], les agences chargées des poursuites, les autres agences de justice pénale et les autres titulaires ou organisations qui exercent des activités répressives. Parmi ces derniers, l'annexe 7 de la DPA 2018 cite les procureurs généraux du Royaume-Uni (Directors of Public Prosecutors), le directeur des poursuites pénales en Irlande du Nord (Director of Public Prosecutors for Northern Ireland) ou la commission de l'information (Information Commission).

communications (Government Communications Headquarters)] ne sont pas des «autorités compétentes»[134] au sens de la partie 3 de la DPA 2018 et, par conséquent, les règles qui y sont définies ne s'appliquent à aucune de leurs activités. Une partie spécifique de la DPA 2018 (partie 4) est consacrée au traitement des données à caractère personnel par les services de renseignement (pour plus de détails, voir le considérant (125)).

(124) À l'instar de la directive (UE) 2016/680, la partie 3 de la DPA 2018 énonce les principes de licéité et de loyauté[135], de limitation de la finalité[136], de minimisation des données[137], d'exactitude[138], de limitation de la conservation[139] et de sécurité[140]. La législation impose des obligations spécifiques de transparence[141] et confère aux personnes concernées un droit d'accès[142], de rectification et de suppression[143] et le droit de ne pas faire l'objet d'une prise de décision automatisée[144]. Les autorités compétentes doivent également mettre en œuvre des mesures de protection des données dès la conception et par défaut, tenir un registre des activités de traitement et, pour certaines opérations de traitement, effectuer des analyses d'impact relatives à la protection des données et consulter au préalable le commissaire à l'information[145]. Conformément à l'article 56 de la DPA 2018, elles sont tenues de démontrer la conformité du traitement. En outre, les autorités compétentes doivent mettre en place des mesures appropriées visant à garantir la sécurité du traitement[146] et elles sont soumises à des obligations spécifiques en cas de violation de données, notamment l'obligation de notifier une telle violation au commissaire à l'information et aux personnes concernées[147]. À l'instar de ce que dispose la directive (UE) 2016/680, le responsable du traitement est également tenu (sauf s'il s'agit d'une juridiction ou d'une autre autorité judiciaire agissant dans l'exercice de sa fonction juridictionnelle) de désigner un délégué à la protection des données (DPD)[148] qui l'aidera à se conformer à ses obligations et à contrôler le respect de ces obligations[149]. Par ailleurs, afin de garantir la continuité de la protection, la loi impose des exigences spécifiques relatives aux transferts internationaux des données à caractère personnel à des fins répressives vers des pays tiers ou à des organisations internationales[150]. À la même date que pour la présente décision, la Commission a adopté une décision d'adéquation en vertu de l'article 36, paragraphe 3, de la directive (UE) 2016/680, constatant que le

134 Article 30, paragraphe 2, de la DPA 2018.
135 Article 35 de la DPA 2018.
136 Article 36 de la DPA 2018.
137 Article 37 de la DPA 2018.
138 Article 38 de la DPA 2018.
139 Article 39 de la DPA 2018.
140 Article 40 de la DPA 2018.
141 Article 44 de la DPA 2018.
142 Article 45 de la DPA 2018.
143 Articles 46 et 47 de la DPA 2018.
144 Articles 49 et 50 de la DPA 2018.
145 Articles 56 à 65 de la DPA 2018.
146 Article 66 de la DPA 2018.
147 Articles 67 et 68 de la DPA 2018.
148 Articles 69 à 71 de la DPA 2018.
149 Articles 67 et 68 de la DPA 2018.
150 Partie 3, chapitre 5, de la DPA 2018.

régime de protection des données applicable au traitement des données par les autorités répressives britanniques assure un niveau de protection essentiellement équivalent à celui garanti par la directive (UE) 2016/680.

(125) La partie 4 de la DPA 2018 s'applique à l'ensemble des traitements par les services de renseignement ou pour le compte de ces derniers. Elle énonce notamment les grands principes relatifs à la protection des données (licéité, loyauté et transparence[151]; limitation de la finalité[152], minimisation des données[153], exactitude[154]; limitation de la conservation[155] et sécurité[156]), impose des conditions au traitement de catégories particulières de données[157], établit les droits des personnes concernées[158], exige la protection des données dès la conception[159] et réglemente les transferts internationaux de données à caractère personnel[160]. L'ICO a récemment publié des orientations

151 En vertu de l'article 86, paragraphe 6, de la DPA 2018, pour déterminer la loyauté et la transparence du traitement, il convient de prendre en considération la méthode d'obtention des données. En ce sens, l'exigence de loyauté et de transparence est remplie si les données ont été obtenues auprès d'une personne légalement habilitée à les fournir ou légalement tenue de les fournir.

152 Conformément à l'article 87 de la DPA 2018, les finalités du traitement doivent être déterminées, explicites et légitimes. Les données ne doivent pas être traitées d'une manière incompatible avec les finalités pour lesquelles elles sont collectées. En vertu de l'article 87, paragraphe 3, de la DPA 2018, tout autre traitement compatible de données à caractère personnel n'est permis que si le responsable du traitement est autorisé par la loi à traiter les données à cette fin et si le traitement est nécessaire et proportionné à cette autre finalité. Il y a lieu de considérer le traitement comme compatible s'il est effectué à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, et s'il fait l'objet de garanties appropriées (article 87, paragraphe 4, de la DPA 2018).

153 Les données à caractère personnel doivent être adéquates, pertinentes et limitées (article 88 de la DPA 2018).

154 Les données à caractère personnel doivent être exactes et à jour (article 89 de la DPA 2018).

155 Les données à caractère personnel ne doivent pas être conservées plus longtemps que nécessaire (article 90 de la DPA 2018).

156 Le sixième principe en matière de protection des données est que les données à caractère personnel doivent être traitées d'une manière qui consiste notamment à prendre des mesures de sécurité appropriées au regard des risques que présente le traitement de ces données. Ces risques incluent (entre autres) la destruction, la perte, l'utilisation, la modification ou la divulgation de données à caractère personnel, ou l'accès à de telles données, de manière accidentelle ou illicite (article 91 de la DPA 2018). L'article 107 exige également a) que chaque responsable du traitement mette en œuvre des mesures de sécurité appropriées au regard des risques découlant du traitement des données à caractère personnel et 2) dans le cas d'un traitement automatisé, que chaque responsable du traitement et chaque sous-traitant mettent en œuvre des mesures de prévention ou d'atténuation fondées sur une évaluation du risque.

157 Article 86, paragraphe 2, point b), et annexe 10 de la DPA 2018.

158 Partie 4, chapitre 3, de la DPA 2018, notamment les droits: d'accès, de rectification et de suppression, de s'opposer au traitement et de ne pas faire l'objet d'une prise de décision automatisée, d'intervenir dans une prise de décision automatisée et d'être informée de la prise de décision. En outre, le responsable du traitement doit informer la personne concernée du traitement des données à caractère personnel la concernant. Comme expliqué dans les orientations de l'ICO sur le traitement par les services de renseignement, les personnes physiques peuvent exercer tous leurs droits (y compris une demande de rectification) en déposant une plainte auprès de l'ICO ou en saisissant les tribunaux (voir les orientations de l'ICO sur le traitement des services de renseignement, disponibles à l'adresse suivante: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-intelligence-services-processing/).

159 Article 103 de la DPA 2018.

160 Article 109 de la DPA 2018. Les transferts de données à caractère personnel à des organisations internationales ou vers des pays en dehors du Royaume-Uni sont possibles si le transfert constitue une mesure nécessaire et proportionnée mise en œuvre aux fins de l'exercice des pouvoirs réglementaires du

détaillées sur le traitement par les services de renseignement au titre de la partie 4 de la DPA 2018[161].

(126) Dans le même temps, l'article 110 de la DPA 2018 prévoit une exemption à certaines dispositions spécifiques de la partie 4[162] lorsque ladite exemption est nécessaire pour garantir la sécurité nationale. Cette exemption peut être appliquée sur la base d'une analyse au cas par cas[163]. Comme expliqué par les autorités britanniques et confirmé par la jurisprudence, un «responsable du traitement doit considérer les conséquences concrètes pour la sécurité nationale ou la défense s'il devait respecter la disposition particulière relative à la protection des données, et s'il pouvait raisonnablement respecter la règle habituelle sans porter atteinte à la sécurité ou à la défense nationale»[164]. La question de savoir si l'exemption a été appliquée de manière appropriée est soumise à la surveillance de l'ICO[165].

(127) Par ailleurs, en ce qui concerne la possibilité de limiter, aux fins de la protection de la «sécurité nationale», l'application des dispositions spécifiques susmentionnées, conformément à l'article 111 de la DPA 2018, un responsable du traitement peut demander un certificat signé par un ministre du cabinet ou par le procureur général attestant qu'une limitation de ces droits constitue une mesure nécessaire et proportionnée à la protection de la sécurité nationale[166].

---

responsable du traitement ou à d'autres fins prévues dans des articles spécifiques de la loi de 1989 sur les services de sécurité et de la loi de 1994 sur les services de renseignement.

161 Orientations de l'ICO, voir note de bas de page 158.

Article 30 et annexe 7 de la DPA 2018.

162 L'article 110, paragraphe 2, de la DPA 2018 énumère les dispositions auxquelles une exemption est autorisée. Ces dispositions incluent les principes relatifs à la protection des données (à l'exception du principe de licéité), les droits des personnes concernées, l'obligation d'informer le commissaire à l'information de toute violation de données, les pouvoirs d'inspection du commissaire à l'information conformément aux obligations internationales et certains de ses pouvoirs d'application des règles, les dispositions assimilant certaines violations de la protection des données à des infractions pénales et les dispositions relatives à des finalités particulières de traitement, comme les finalités journalistiques, universitaires ou artistiques.

163 Voir l'arrêt Baker/Secretary of State, note de bas de page 61.

164 Cadre explicatif relatif aux discussions sur l'adéquation du Royaume-Uni, section H: Cadre de la sécurité nationale, de la protection des données et des pouvoirs d'enquête, p. 15 et 16 (voir la note de bas de page 31). Voir également l'arrêt Baker/Secretary of State (note de bas de page 61) dans lequel le tribunal a annulé un certificat de sécurité nationale délivré par le ministre de l'intérieur et confirmant l'application de l'exception relative à la sécurité nationale, estimant qu'il n'y avait aucune raison d'appliquer une exception générale à l'obligation de répondre aux demandes d'accès et que l'autorisation d'une telle exception en toutes circonstances, sans une analyse au cas par cas, dépassait ce qui était nécessaire et proportionné à la protection de la sécurité nationale.

165 Voir le protocole d'accord entre l'ICO et la communauté du renseignement britannique (UKIC) en vertu duquel «lorsqu'il reçoit une réclamation d'une personne concernée, l'ICO voudra s'assurer que le problème a été correctement traité et, le cas échéant, que l'application d'une exemption a été effectuée de façon appropriée». Protocole d'accord entre le Bureau du commissaire à l'information et la communauté du renseignement britannique, point 16, disponible à l'adresse suivante: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf.

166 La DPA 2018 a supprimé la possibilité de délivrer des certificats au titre de l'article 28, paragraphe 2, de la DPA 1998. Toutefois, la possibilité de délivrer d'«anciens certificats» existe toujours, dans la mesure où il existe une action en justice historique en vertu de la loi de 1998 (voir paragraphe 17 de la partie 5 de l'annexe 20 de la DPA 2018). Cette possibilité, toutefois, semble très rare et ne s'appliquera que dans des cas limités, comme, par exemple, lorsque la personne concernée forme un recours contre l'utilisation de l'exception de la sécurité nationale ayant trait à un traitement effectué par une autorité nationale au titre de la loi de 1998. Il y a lieu de noter que dans ces cas, l'article 28 de la DPA 1998

(128) Le gouvernement britannique a publié des orientations afin d'aider les responsables du traitement à déterminer s'il y a lieu de demander un certificat de sécurité nationale au titre de la DPA 2018, qui soulignent notamment que toute limitation des droits des personnes concernées pour garantir la sécurité nationale doit être proportionnée et nécessaire[167]. Tous les certificats de sécurité nationale doivent être publiés sur le site internet de l'ICO[168].

(129) Le certificat devrait être délivré pour une durée déterminée n'excédant pas cinq ans, afin d'être régulièrement examiné par le pouvoir exécutif[169]. Un certificat désigne les données à caractère personnel ou les catégories de données à caractère personnel faisant l'objet de l'exemption, ainsi que les dispositions de la DPA 2018 auxquelles s'applique l'exemption[170].

(130) Il y a lieu de noter que les certificats de sécurité nationale n'ajoutent pas une nouvelle compétence limitant les droits en matière de protection des données à des fins de sécurité nationale. En d'autres termes, le responsable du traitement ou le sous-traitant ne peut se fonder sur un certificat que lorsqu'il a conclu qu'il était nécessaire d'appliquer l'exemption concernant la sécurité nationale, selon une analyse au cas par cas comme expliqué ci-dessus[171]. Même si un certificat de sécurité nationale s'applique à la matière concernée, l'ICO peut examiner si l'application de l'exemption concernant la sécurité nationale était justifiée ou non dans un cas particulier[172].

(131) Toute personne directement concernée par la délivrance d'un certificat peut former un recours devant le tribunal supérieur[173] contre le certificat[174] ou, lorsque ce dernier énumère les données au moyen d'une description générale, contester l'application du

---

s'appliquera dans son ensemble, y compris par conséquent la possibilité pour la personne concernée de contester le certificat devant les tribunaux.

167 Orientations du gouvernement britannique sur les certificats de sécurité nationale au titre de la loi de 2018 sur la protection des données, disponibles à l'adresse suivante: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf. D'après les explications fournies par les autorités britanniques, même si un certificat constitue une preuve déterminante que l'exemption est applicable en ce qui concerne les données ou le traitement décrit dans le certificat, il ne supprime pas l'obligation, pour le responsable du traitement, d'examiner au cas par cas s'il est nécessaire d'appliquer l'exemption.

168 Conformément à l'article 130 de la DPA 2018, l'ICO peut décider de ne pas publier tout ou partie du texte du certificat s'il va à l'encontre de l'intérêt de la sécurité nationale ou s'il est contraire à l'intérêt public ou encore est susceptible de compromettre la sécurité de quiconque. Dans ces cas, l'ICO rendra toutefois public le fait que le certificat a été publié.

169 Orientations du gouvernement britannique sur les certificats de sécurité nationale, point 15, voir la note de bas de page 167.

170 Orientations du gouvernement britannique sur les certificats de sécurité nationale, point 5, voir la note de bas de page 167.

171 Voir la note de bas de page 164.

172 En vertu de l'article 102 de la DPA 2018, le responsable du traitement doit être en mesure de démontrer qu'il s'est conformé à la DPA 2018. Cela signifie qu'un service de renseignement serait tenu de démontrer à l'ICO que, au moment de recourir à l'exemption, il a examiné les circonstances particulières du cas d'espèce. L'ICO a également publié un registre des certificats de sécurité nationale, disponible à l'adresse suivante: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/

173 Le Tribunal supérieur est la juridiction compétente pour connaître des recours contre les décisions rendues par les tribunaux administratifs inférieurs et est expressément compétent en ce qui concerne les recours directs contre les décisions de certains organismes publics.

174 Article 111, paragraphe 3, de la DPA 2018.

certificat à des données spécifiques[175]. Le tribunal examinera la décision de délivrer un certificat et déterminera s'il existait des motifs raisonnables de le délivrer[176]. Il peut examiner divers éléments, notamment la nécessité, la proportionnalité et la licéité du certificat, compte tenu de son incidence sur les droits des personnes concernées et de sa mise en balance avec la nécessité de garantir la sécurité nationale. À l'issue de cet examen, le tribunal peut décider que le certificat ne s'applique pas aux données à caractère personnel spécifiques faisant l'objet du recours[177].

(132) Différentes limitations possibles concernent celles qui s'appliquent, en vertu de l'annexe 11 de la DPA 2018, à certaines dispositions de la partie 4 de la DPA 2018[178] pour garantir d'autres objectifs importants d'intérêt public général ou des intérêts protégés, tels que l'immunité parlementaire, le secret professionnel, le déroulement des procédures judiciaires ou l'efficacité au combat des forces armées[179]. L'application de ces dispositions est soit exemptée pour certaines catégories d'informations (ci-après une exemption «fondée sur une catégorie»), soit exemptée dans la mesure où elle serait susceptible de porter préjudice à l'intérêt protégé (ci-après une exemption «fondée sur un préjudice»)[180]. Les exemptions fondées sur un préjudice ne peuvent

---

175 Article 111, paragraphe 5, de la DPA 2018.

176 Dans l'arrêt *Baker/Secretary of State* (voir la note de bas de page 61), le tribunal de l'information a annulé un certificat de sécurité nationale délivré par le ministre de l'intérieur, estimant qu'il n'y avait aucune raison d'appliquer une exception générale à l'obligation de répondre aux demandes d'accès et que l'autorisation d'une telle exception en toutes circonstances, sans une analyse au cas par cas, dépassait ce qui était nécessaire et proportionné à la protection de la sécurité nationale.

177 Orientations du gouvernement britannique sur les certificats de sécurité nationale, point 25, voir la note de bas de page 167.

178 Il s'agit notamment i) des principes relatifs à la protection des données visés à la partie 4, à l'exception de l'exigence relative à la licéité du traitement prévue par le premier principe et du fait que le traitement doit remplir l'une des conditions pertinentes énoncées aux annexes 9 et 10; ii) des droits des personnes concernées; et iii) des obligations de notification des violations à l'ICO.

179 La partie 4 de la DPA 2018 prévoit le cadre juridique applicable à tout type de traitement de données à caractère personnel réalisé par des agences de renseignement (et non seulement dans l'exercice de leurs missions de sécurité nationale). C'est pourquoi la partie 4 s'applique aussi lorsque des agences de renseignement traitent, par exemple, des données à des fins de gestion des ressources humaines, dans le cadre d'un litige ou dans le contexte de marchés publics. Les limitations énumérées à l'annexe 11 visent principalement à s'appliquer à ces autres contextes. Par exemple, dans le contexte d'un litige avec un salarié, la limitation à des fins de «procédures judiciaires» peut être invoquée, ou dans le contexte des marchés publics, la limitation à des fins de «négociation» peut être invoquée, etc. C'est ce qui ressort des orientations de l'ICO sur le traitement par les services de renseignement, qui mentionnent la négociation d'un règlement entre une agence de renseignement et un ancien salarié faisant valoir une créance découlant d'une relation d'emploi comme un exemple de l'application des limitations prévues à l'annexe 11 (voir la note de bas de page 161). Il y a également lieu de noter que les mêmes limitations sont disponibles pour d'autres autorités publiques, conformément à l'annexe 2 de la partie 2 de la DPA 2018.

180 Selon le cadre explicatif du Royaume-Uni, les exceptions «fondées sur une catégorie» sont les suivantes: i) les informations concernant l'attribution par la Couronne d'une distinction honorifique ou d'un titre de noblesse; ii) le secret professionnel; iii) les références confidentielles en matière d'emploi, de formation ou d'éducation; et iv) les copies et les notes d'examen. Les exceptions «fondées sur un préjudice» concernent les questions suivantes: i) la prévention ou la détection des infractions pénales, l'arrestation ou la poursuite des criminels; ii) l'immunité parlementaire; iii) les procédures judiciaires; iv) l'efficacité au combat des forces armées de la Couronne; v) le bien-être économique du Royaume-Uni; vi) les négociations avec la personne concernée; vii) les finalités de recherche scientifique ou historique, ou les finalités statistiques; viii) les finalités archivistiques dans l'intérêt public. Cadre explicatif relatif aux discussions sur l'adéquation du Royaume-Uni, section H: Sécurité nationale, p. 13, voir la note de bas de page 31.

être invoquées que dans la mesure où l'application de la disposition énumérée relative à la protection des données porterait préjudice à l'intérêt spécifique en question. L'application d'une exemption doit donc toujours être justifiée par la référence au préjudice qui serait susceptible de naître dans chaque cas. Les exemptions fondées sur une catégorie ne peuvent être invoquées qu'en ce qui concerne la catégorie particulière d'informations, définie de manière précise, pour laquelle l'exemption est accordée. Ces exemptions ont un objectif et des effets similaires à ceux de plusieurs exceptions au RGPD britannique (prévues à l'annexe 2 de la DPA 2018), lesquelles correspondent à celles prévues à l'article 23 du RGPD.

(133) Il ressort de ce qui précède que les dispositions juridiques britanniques applicables, telles qu'elles ont été également interprétées par les juridictions et le commissaire à l'information, prévoient bien des limitations et des conditions pour garantir que les exemptions et les limitations susmentionnées restent dans les limites de ce qui est nécessaire et proportionné à la protection de la sécurité nationale.

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

(134) Le droit du Royaume-Uni impose un certain nombre de limitations à l'accès aux données à caractère personnel et à l'utilisation de celles-ci à des fins répressives. Il prévoit également des mécanismes de surveillance et de recours dans ce domaine qui sont conformes aux exigences visées aux considérants (113) à (115) de la présente décision. Les conditions dans lesquelles un tel accès peut intervenir et les garanties applicables à l'utilisation de ces pouvoirs sont évaluées en détail dans les sections suivantes.

3.2.1 Bases juridiques et limitations/garanties applicables

(135) Conformément au principe de licéité garanti en vertu de l'article 35 de la DPA 2018, le traitement des données à caractère personnel pour l'une des finalités répressives n'est licite que s'il est fondé sur le droit et si la personne concernée a donné son consentement au traitement pour cette finalité[181] ou si le traitement est nécessaire à l'exécution d'une mission exercée à cette fin par une autorité compétente.

3.2.1.1 Mandats de perquisition et injonctions de production

(136) Dans le cadre juridique du Royaume-Uni, la collecte des données à caractère personnel auprès des opérateurs économiques, y compris ceux qui traiteraient des données transférées depuis l'UE au titre de la présente décision d'adéquation, à des fins répressives est autorisée sur la base de mandats de perquisition[182] et d'injonctions de production[183].

---

181 L'utilisation du consentement ne semble pas pertinente dans un scénario d'adéquation dans la mesure où, dans une situation de transfert, les données n'auront pas été directement collectées auprès d'une personne concernée de l'Union par une autorité répressive britannique sur la base du consentement.

182 S'agissant de la base juridique applicable, voir les articles 8 et suivants de la loi de 1984 sur la police et les preuves criminelles (pour l'Angleterre et le pays de Galles) (PACE 1984), les articles 10 et suivants de l'ordonnance de 1989 sur la police et les preuves criminelles (pour l'Irlande du Nord). Pour l'Écosse, le mandat est obtenu en vertu de la common law [voir l'article 46 de la loi écossaise de 2016 sur la justice pénale) et l'article 23B de la loi écossaise de 1995 sur le droit pénal (consolidation)]. S'agissant des mandats de perquisition délivrés après l'arrestation, la base juridique est constituée par l'article 18 de la PACE 1984 (pour l'Angleterre et le pays de Galles) et les articles 20 et suivants de l'ordonnance de 1989 sur la police et les preuves criminelles (pour l'Irlande du Nord). Pour l'Écosse, le mandat est obtenu en vertu de la common law (voir l'article 46 de la loi écossaise de 2016 sur la justice pénale).

(137) Les mandats de perquisition sont délivrés par un tribunal, généralement à la demande de l'enquêteur. Ils autorisent un enquêteur à pénétrer dans des locaux afin de rechercher des personnes ou des éléments pertinents pour son enquête et à conserver tout élément pour lequel une perquisition a été autorisée, y compris les documents ou les pièces contenant des données à caractère personnel[184]. Une injonction de production, qui doit être également délivrée par un tribunal, oblige la personne désignée dans celle-ci à produire les éléments qui sont en sa possession ou sous son contrôle, ou à donner accès à ceux-ci. Le requérant doit expliquer au tribunal les raisons pour lesquelles le mandat ou l'injonction est nécessaire et dans l'intérêt public. Il existe plusieurs pouvoirs réglementaires qui permettent de délivrer des mandats de perquisition et des injonctions de production. Chaque disposition contient son propre ensemble de conditions légales qui doivent être satisfaites aux fins de la délivrance d'un mandat de perquisition[185] ou d'une injonction de production[186].

Les autorités britanniques ont précisé que les mandats de perquisition étaient délivrés par un tribunal, à la demande de l'enquêteur. Ils autorisent un enquêteur à pénétrer dans des locaux afin de rechercher des personnes ou des éléments pertinents pour son enquête; l'exécution du mandat nécessitera souvent l'assistance d'un officier de police judiciaire.

183 Lorsque l'enquête porte sur le blanchiment de capitaux (y compris dans le cadre de procédures de confiscation et de récupération), la base juridique pertinente pour les demandes d'injonction de production est constituée par les articles 345 et suivants de la loi de 2002 sur les produits du crime (pour l'Angleterre, le pays de Galles et l'Irlande du Nord) et les articles 380 et suivants de la loi de 2002 sur les produits du crime pour l'Écosse. Lorsque l'enquête porte sur d'autres questions que le blanchiment de capitaux, une demande d'injonction de production peut être introduite au titre de l'article 9 et de l'annexe 1 de la PACE 1984 pour l'Angleterre et le pays de Galles, et des articles 10 et suivants de l'ordonnance d'Irlande du Nord de 1989 sur la police et les preuves criminelles pour l'Irlande du Nord. Pour l'Écosse, l'injonction est obtenue en vertu de la *common law* [voir l'article 46 de la loi écossaise de 2016 sur la justice pénale et l'article 23B de la loi écossaise sur le droit pénal (consolidation)]. Les autorités britanniques ont précisé qu'une injonction de production obligeait la personne désignée dans celle-ci à produire les éléments qui sont en sa possession ou sous son contrôle, ou à donner accès à ceux-ci (voir l'annexe 1, point 4, de la PACE 1984).

184 Par exemple, les pouvoirs de saisir et de conserver tout élément pour lequel une perquisition a été autorisée sont visés aux articles 8 et 18 de la PACE 1984.

185 Par exemple, les articles 8 et 18 de la PACE réglementent respectivement le pouvoir d'un juge de paix d'autoriser un mandat et le pouvoir d'un agent de police de perquisitionner une propriété. Dans le premier cas (article 8), avant de délivrer un mandat, un juge de paix doit en premier lieu s'assurer qu'il existe des motifs raisonnables de croire: i) qu'une infraction majeure a été commise; ii) que les locaux abritent des éléments susceptibles d'être importants (individuellement ou en combinaison avec d'autres éléments) aux fins de l'enquête portant sur l'infraction; iii) que ces éléments sont susceptibles de constituer des preuves pertinentes; iv) qu'il ne s'agit pas d'éléments couverts par le secret professionnel, d'éléments exclus ou d'éléments relevant d'une procédure spéciale; et v) qu'il ne serait pas possible de pénétrer dans les lieux sans utiliser un mandat. Dans le deuxième cas, l'article 18 autorise un agent de police à effectuer une perquisition dans les locaux d'une personne arrêtée pour une infraction majeure afin de rechercher des éléments autres que des éléments couverts par le secret professionnel, s'il a des motifs raisonnables de suspecter que les locaux abritent des éléments de preuve relatifs à cette infraction ou à une autre infraction majeure, similaire ou connexe. Une telle perquisition doit se limiter à la recherche de ces éléments et doit être autorisée, par écrit, par un agent de police de grade au moins égal à celui de brigadier-chef, à moins que cela ne soit nécessaire aux fins de l'enquête portant sur l'infraction. Auquel cas, un agent de grade au moins égal à celui de brigadier-chef doit être informé dès que possible après que la perquisition a été effectuée. Les motifs de la perquisition et la nature des preuves recherchées doivent être consignés par écrit. De plus, les articles 15 et 16 de la PACE 1984 prévoient des garanties légales qui doivent être respectées en cas de demande d'un mandat de perquisition. L'article 15 énonce les exigences applicables à l'obtention d'un mandat de perquisition (notamment le contenu de la demande introduite par l'officier et le fait que le mandat doit préciser, entre autres choses, la disposition législative en vertu de laquelle il est délivré et indiquer, dans la mesure du possible, les éléments et les personnes à rechercher, ainsi que les locaux à perquisitionner). L'article 16

(138) Les injonctions de production et les mandats de perquisition peuvent être contestés par la voie du contrôle juridictionnel[187]. En matière de garanties, toutes les autorités

---

régit la façon dont une perquisition doit se dérouler dans le cadre d'un mandat (par exemple: l'article 16, paragraphe 5, prévoit que l'agent chargé d'exécuter le mandat remet à l'occupant une copie du mandat; l'article 16, paragraphe 11, dispose que le mandat, une fois exécuté, doit être conservé pour une durée de 12 mois; l'article 16, paragraphe 12, confère à l'occupant le droit d'examiner le mandat au cours de cette période s'il le souhaite). Ces articles contribuent à assurer le respect de l'article 8 de la CEDH [voir par exemple l'arrêt du président de la Haute Cour Kent Pharmaceuticals/Director of the Serious Fraud Office [2002] EWHC 3023 (QB), point 30]. La perquisition peut être déclarée illégale en cas de non-respect de ces garanties [c'est le cas, par exemple, dans les arrêts R (Brook)/Preston Crown Court [2018] EWHC 2024 (Admin), [2018] ACD 95; R (Superior Import/Export Ltd)/Revenue and Customs Commissioners [2017] EWHC 3172 (Admin), [2018] Lloyd's Rep FC 115; et R (F)/Blackfriars Crown Court [2014] EWHC 1541 (Admin)]. Les articles 15 et 16 de la PACE 1984 sont complétés par son code B, un code de bonnes pratiques qui régit l'exercice des pouvoirs policiers aux fins de la perquisition de locaux.

186 Par exemple, lors de la délivrance d'une injonction de production au titre de la loi de 2002 sur les produits du crime, outre les motifs raisonnables nécessaires pour remplir les conditions énoncées à l'article 346, paragraphe 2, de la loi sur les produits du crime, il doit exister des motifs raisonnables de suspecter que les éléments recherchés sont en la possession de la personne ou sous son contrôle et qu'ils sont susceptibles d'être importants. Par ailleurs, pour qu'une injonction de production soit délivrée, il doit exister des motifs raisonnables de penser qu'il est dans l'intérêt public de produire les éléments ou de donner accès à ceux-ci, au vu a) de l'avantage pour l'enquête susceptible de découler de l'obtention de ces éléments; et b) des circonstances dans lesquelles, selon la demande, la personne semble être en possession ou avoir le contrôle des éléments contenant ses informations. De même, un tribunal étudiant une demande d'injonction de production introduite au titre de l'annexe 1 de la PACE 1984 doit s'assurer du respect de certaines conditions. L'annexe 1 de la PACE décrit notamment deux ensembles alternatifs distincts de conditions, dont l'un doit être rempli avant qu'un juge puisse délivrer une injonction de production. Selon les exigences du premier ensemble, le juge doit avoir des motifs raisonnables de penser i) qu'une infraction majeure a été commise; ii) que les éléments recherchés dans les locaux consistent en, ou incluent, des éléments relevant d'une procédure spéciale, mais non exclus; iii) qu'ils sont susceptibles d'être importants, individuellement ou en combinaison avec d'autres éléments, aux fins de l'enquête; iv) et qu'ils sont susceptibles de constituer des preuves pertinentes; v) que d'autres méthodes pour obtenir ces éléments ont été tentées ou n'ont pas été tentées car elles étaient vouées à l'échec; et vi) que, compte tenu des avantages pour l'enquête et des circonstances dans lesquelles la personne est en possession des éléments, il est dans l'intérêt public de produire ces éléments ou de donner accès à ceux-ci. Les exigences du deuxième ensemble de conditions sont les suivantes: i) les locaux abritent des éléments qui consistent en des éléments relevant d'une procédure spéciale ou exclus; ii) si ce n'était l'interdiction frappant les perquisitions effectuées sur la base de la législation adoptée avant la PACE pour rechercher des éléments exclus, relevant d'une procédure spéciale ou couverts par le secret professionnel, un mandat de perquisition pour ces éléments aurait pu être délivré; et iii) la délivrance d'un tel mandat aurait été appropriée.

187 Le contrôle juridictionnel désigne la procédure juridique par laquelle les décisions d'un organisme public peuvent être contestées devant la Haute Cour. La Cour «examine» la décision contestée et détermine si l'argument selon lequel la décision est juridiquement erronée au regard des concepts/principes de droit public est recevable ou non. Les motifs de base d'un contrôle juridictionnel sont l'illégalité, l'irrationalité, un vice de forme, des attentes légitimes et les droits de l'homme. Après qu'un contrôle juridictionnel a confirmé le caractère erroné d'une décision, une juridiction est en mesure de prononcer différentes mesures correctrices; il s'agit le plus souvent d'une ordonnance d'annulation (qui annule la décision initiale, à savoir la décision de délivrer un mandat de perquisition) et, dans certains cas, ces mesures peuvent également inclure l'octroi d'un dédommagement financier. De plus amples informations sur le contrôle juridictionnel au Royaume-Uni figurent dans la publication du service juridique du gouvernement intitulée «Judge Over Your Shoulder – a guide to good decision-making», disponible à l'adresse suivante:

répressives en matière pénale relevant du champ d'application de la partie 3 de la DPA 2018, y compris la police, ne peuvent accéder à des données à caractère personnel (ce qui est en soi une forme de traitement) que dans le respect des principes et des exigences énoncés dans cette loi [voir les considérants (122) et (124) above]. Par conséquent, une demande introduite par une autorité répressive devrait respecter le principe selon lequel les finalités du traitement doivent être déterminées, explicites et légitimes[188] et les données à caractère personnel traitées par une autorité compétente doivent être pertinentes et limitées au regard de ces finalités[189].

3.2.1.2 Pouvoirs d'enquête à des fins répressives

(139) Aux fins de la prévention ou de la détection des seules infractions graves[190], certaines autorités répressives, comme, par exemple, l'Agence nationale de lutte contre la criminalité ou le chef de la police[191], peuvent exercer des pouvoirs d'enquête ciblés au titre de l'IPA 2016. Dans ce cas, les garanties prévues par l'IPA 2016 s'appliqueront en plus de celles prévues par la partie 3 de la DPA 2018. 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), la conservation de données de communication (partie 4 de l'IPA 2016) et l'interférence ciblée avec des équipements (partie 5 de l'IPA 2016). L'interception d'une communication recouvre l'acquisition du contenu d'une communication[192], tandis que l'acquisition et la conservation de données de communication visent non pas à obtenir le contenu de la communication, mais à déterminer le «qui», le «quand», le «où» et le «comment» de la communication. Il s'agit, par exemple, de l'heure et de la durée d'une communication, du numéro de téléphone ou de l'adresse électronique de l'expéditeur et du destinataire de la communication, et parfois de la localisation des appareils à partir desquels la communication a été effectuée, de l'abonné à un service téléphonique ou d'une facture détaillée.[193] L'interférence avec des équipements est un

---

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746170/JOYS-OCT-2018.pdf.

188 Article 36, paragraphe 1, de la DPA 2018.

189 Article 37 de la DPA 2018.

190 Conformément à l'article 263, paragraphe 1, de l'IPA 2016, on entend par «infraction grave» une infraction pour laquelle un adulte qui n'a fait l'objet d'aucune condamnation antérieure pourrait raisonnablement s'attendre à être condamné à une peine d'emprisonnement d'une durée égale ou supérieure à trois ans, ou qui implique l'usage de la violence, qui entraîne un gain financier important ou qui est commise par un grand nombre de personnes. En outre, aux fins de l'acquisition des données de communication au titre de la partie 4 de l'IPA 2016, conformément à l'article 87, paragraphe 10B, on entend par «infraction grave» une infraction passible d'une peine d'emprisonnement d'une durée égale ou supérieure à douze mois ou une infraction commise par une personne qui n'est pas une personne physique ou qui comporte, en tant que composante à part entière, l'envoi d'une communication ou une violation de la vie privée d'une personne.

191 Les autorités répressives suivantes peuvent notamment demander un mandat d'interception ciblée: le directeur général de l'Agence nationale de lutte contre la criminalité, le commissaire de la police métropolitaine, le préfet de police du service de police d'Irlande du Nord, le préfet de police du service de police d'Écosse, le commissaire de l'administration fiscale et douanière du Royaume-Uni, le chef du renseignement de la défense et une personne qui est une autorité compétente d'un pays ou d'un territoire situé en dehors du Royaume-Uni aux fins d'un instrument d'assistance mutuelle de l'UE ou d'un accord international d'entraide judiciaire (article 18, paragraphe 1, de l'IPA 2016).

192 Voir l'article 4 de l'IPA 2016.

193 Voir l'article 261, paragraphe 5, de l'IPA 2016 et le code de bonnes pratiques relatif à l'acquisition de masse de données de communication, disponible à l'adresse suivante:

ensemble de techniques utilisées afin d'obtenir diverses données à partir d'équipements tels que les ordinateurs, les tablettes et les smartphones, ainsi que les câbles, les fils et les appareils de stockage[194].

(140) Les pouvoirs d'interception ciblée peuvent également être utilisés lorsque cela est «nécessaire aux fins de donner effet aux dispositions d'un instrument d'entraide judiciaire de l'UE ou d'un accord d'entraide judiciaire international» (appelé «mandat d'entraide judiciaire»[195]). Les mandats d'entraide judiciaire ne sont délivrés que dans le cadre de l'interception de communications, et non de l'acquisition de données de communication ou de l'interférence avec des équipements. Ces pouvoirs ciblés sont réglementés par la loi de 2016 sur les pouvoirs d'enquête[196], qui, 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, constituent la base juridique de ces pouvoirs et définissent les limitations et les garanties relatives à l'exercice de ces pouvoirs. L'IPA 2016 prévoit également le régime applicable à l'utilisation des pouvoirs de surveillance de masse, bien que ces derniers ne soient pas accessibles aux autorités répressives (seules les agences de renseignement sont habilitées à les utiliser)[197].

(141) Pour exercer ces pouvoirs, les autorités doivent obtenir un mandat[198] délivré par une autorité compétente[199] et approuvé par un commissaire judiciaire indépendant[200]

---

194 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf, point 2.9.
Code de bonnes pratiques relatif à l'interférence avec des équipements, disponible à l'adresse suivante: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, point 2.2.

195 Un mandat d'entraide judiciaire autorise une autorité britannique à prêter assistance à une autorité située en dehors du Royaume-Uni aux fins de l'interception de communications et de la divulgation des données interceptées à cette autorité, conformément à un instrument international d'entraide judiciaire (article 15, paragraphe 4, de l'IPA 2016).

196 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, à l'interférence avec des 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.

197 Article 138, paragraphe 1, article 158, paragraphe 1, article 178, paragraphe 1 et article 199, paragraphe 1, de l'IPA 2016.

198 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.

199 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 d'interférence ciblée avec des équipements lorsque les personnes ou les locaux visés par l'interception et les équipements concernés par l'interférence sont situés en Écosse (voir les articles 22 et 103 de l'IPA 2016). En cas d'interférence ciblée avec des 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.

200 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 [pour de plus amples informations, voir les considérants (162) et suivants].

(procédure dite «de double verrouillage»). L'obtention de ce mandat est soumise à un critère de nécessité et de proportionnalité[201]. Étant donné que ces pouvoirs d'enquêtes ciblés prévus par l'IPA 2016 sont identiques à ceux des agences de sécurité nationale, les conditions, les limitations et les garanties applicables à ces pouvoirs sont détaillées à la section relative à l'accès aux données à caractère personnel et à l'utilisation de celles-ci par les autorités publiques du Royaume-Uni à des fins de sécurité nationale (voir les considérants (177) et suivants).

3.2.2 Utilisation ultérieure des informations recueillies

(142) 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») est soumis à certaines conditions.

(143) À l'instar de ce que prévoit l'article 4, paragraphe 2, de la directive (UE) 2016/680, l'article 36, paragraphe 3, de la DPA 2018 autorise le traitement ultérieur des données collectées par une autorité compétente à des fins répressives (par le responsable initial du traitement ou par un autre responsable du traitement) pour toute autre finalité répressive, à condition que le responsable du traitement soit autorisé par la loi à traiter ces données pour une telle finalité et que le traitement soit nécessaire et proportionné à cette autre finalité[202]. Dans ce cas, toutes les garanties prévues à la partie 3 de la DPA 2018 et visées aux considérants (122) et (124) s'appliquent au traitement effectué par l'autorité destinataire.

(144) Dans l'ordre juridique britannique, différentes lois autorisent explicitement un tel partage ultérieur. En particulier, i) la loi de 2017 sur l'économie numérique autorise le partage de données entre des autorités publiques à plusieurs fins, par exemple en cas de fraude à l'encontre du secteur public qui entraînerait une perte ou un risque de perte pour les autorités publiques[203] ou en cas de dette auprès d'une autorité publique ou de la Couronne[204]; ii) la loi de 2013 sur la criminalité et les juridictions autorise le partage d'informations avec l'agence nationale de lutte contre la criminalité (National Crime Agency, NCA)[205] dans le cadre de la lutte contre la grande criminalité organisée, ainsi que des enquêtes et des poursuites en la matière; iii) la loi de 2007 sur la grande criminalité permet aux autorités publiques de divulguer des informations aux organisations antifraude à des fins de prévention de la fraude[206].

(145) Ces lois prévoient explicitement que le partage d'informations devrait respecter les principes énoncés dans la DPA 2018. En outre, le collège britannique de la police a publié une pratique professionnelle autorisée concernant le partage d'information[207]s afin d'aider la police à respecter ses obligations en matière de protection des données découlant du RGPD britannique, de la DPA 2018 et de la loi de 1998 sur les droits de

---

201 Voir, en particulier, les articles 19 et 23 de l'IPA 2016.

202 Article 36, paragraphe 3, de la DPA 2018.

203 Article 56 de la loi de 2017 sur l'économique numérique, disponible à l'adresse suivante: https://www.legislation.gov.uk/ukpga/2017/30/section/56

204 Article 48 de la loi de 2017 sur l'économie numérique.

205 Article 7 de la loi de 2013 sur la criminalité et les juridictions, disponible à l'adresse suivante: https://www.legislation.gov.uk/ukpga/2013/22/section/7

206 Article 68 de la loi de 2007 sur les infractions graves, disponible à l'adresse suivante: https://www.legislation.gov.uk/ukpga/2007/27/contents

207 Pratique professionnelle autorisée concernant le partage d'informations, disponible à l'adresse suivante: https://www.app.college.police.uk/app-content/information-management/sharing-police-information

l'homme. La conformité du partage avec le cadre juridique en vigueur en matière de protection des données est naturellement soumise à un contrôle juridictionnel[208].

(146) Par ailleurs, à l'instar de ce que dispose l'article 9 de la directive (UE) 2016/680, la DPA 2018 prévoit que les données à caractère personnel collectées à des fins répressives peuvent être traitées à des fins autres que des fins répressives lorsque le traitement est autorisé par la loi[209].

(147) Ce type de partage concerne deux scénarios: 1) le partage de données par une autorité répressive avec une autorité non répressive autre qu'une agence de renseignement (par exemple une autorité financière ou fiscale, une autorité de la concurrence, un service d'aide sociale à l'enfance, etc.); et 2) le partage de données par une autorité répressive avec une agence de renseignement. Dans le premier scénario, le traitement des données à caractère personnel relève du champ d'application du RGPD britannique, ainsi que de la partie 2 de la DPA 2018. La Commission a évalué les garanties prévues par le RGPD britannique et la partie 2 de la DPA 2018 aux considérants (12) à (111) et a conclu que le Royaume-Uni assurait un niveau de protection adéquat des données à caractère personnel transférées au titre du règlement (UE) 2016/679 de l'Union européenne vers le Royaume-Uni.

(148) Dans le deuxième scénario, en ce qui concerne le partage des données collectées par une autorité répressive avec une agence de renseignement à des fins de sécurité nationale, la base juridique autorisant un tel partage est l'article 19 de la loi de 2008 sur la lutte contre le terrorisme (CTA 2008)[210]. En vertu de cette loi, toute personne peut fournir des informations à un service de renseignement, quel qu'il soit, aux fins de l'exercice de l'une de ses fonctions, notamment à des fins de «sécurité nationale».

(149) S'agissant des conditions dans lesquelles les données peuvent être partagées à des fins de sécurité nationale, la loi sur les services de renseignement[211] et la loi sur les services de sécurité[212] limitent la capacité des services de renseignement à obtenir des données à ce qui est nécessaire aux fins de l'exercice de leurs pouvoirs réglementaires. Les services répressifs qui veulent partager des données avec les services de renseignement devront prendre en considération un certain nombre de facteurs/limitations, outre les pouvoirs réglementaires de ces services qui sont décrits

---

208 Voir à titre d'exemple l'affaire M, R/the Chief Constable of Sussex Police [2019] EWHC 975 (Admin) dans laquelle il a été demandé à la Haute Cour d'examiner le partage de données entre la police et le BCRP (Business Crime Reduction Partnership), une organisation habilitée à gérer les régimes des avis de bannissement interdisant à des personnes de pénétrer dans les locaux commerciaux de ses membres. La Cour a examiné le partage de données, qui a eu lieu sur la base d'un accord visant à la protection du public et à la prévention de la criminalité, et a finalement conclu que la plupart des aspects du partage de données étaient licites, sauf en ce qui concerne certaines informations sensibles échangées entre la police et le BCRP. Voir également à titre d'exemple l'affaire Cooper/NCA [2019] EWCA Civ 16 dans laquelle la Cour d'appel a confirmé la licéité du partage de données entre la police et l'agence de lutte contre la grande criminalité organisée (SOCA), une autorité répressive qui fait actuellement partie de la NCA.

209 Article 36, paragraphe 4, de la DPA 2018.

210 Loi de 2008 sur la lutte contre le terrorisme, disponible à l'adresse suivante: https://www.legislation.gov.uk/ukpga/2008/28/section/19.

211 Loi de 1994 sur les services de renseignement, disponible à l'adresse suivante: https://www.legislation.gov.uk/ukpga/1994/13/contents.

212 Loi de 1989 sur les services de sécurité, disponible à l'adresse suivante: https://www.legislation.gov.uk/ukpga/1989/5/contents.

dans la loi sur les services de renseignement et la loi sur les services de sécurité[213]. L'article 20 de la CTA 2008 établit clairement que tout partage de données conforme à l'article 19 doit néanmoins respecter la législation relative à la protection des données; autrement dit, l'ensemble des limitations et des exigences prévues à la partie 3 de la DPA 2018 s'applique. En outre, dans la mesure où les autorités compétentes sont des autorités publiques au sens de la loi de 1998 sur les droits de l'homme, elles doivent veiller à agir dans le respect des droits reconnus par la convention, notamment l'article 8 de la CEDH. Ces limitations garantissent que tout partage de données entre les services répressifs et les services de renseignement respecte la législation relative à la protection des données et la CEDH.

(150) Lorsqu'une autorité compétente envisage de partager des données à caractère personnel traitées au titre de la partie 3 de la DPA 2018 avec les autorités répressives d'un pays tiers, des exigences spécifiques s'appliquent[214]. En particulier, ces transferts peuvent avoir lieu lorsqu'ils sont fondés sur des règlements d'adéquation adoptés par le secrétaire d'État ou, en l'absence de tels règlements, lorsque des garanties appropriées sont prévues. L'article 75 de la DPA 2018 prévoit que des garanties appropriées sont en place lorsqu'elles ont été instaurées par un instrument juridique contraignant pour le destinataire prévu, ou lorsque le responsable du traitement, après avoir apprécié l'ensemble des circonstances entourant les transferts de ce type de données à caractère personnel vers le pays tiers ou à l'organisation internationale concernée, conclut que des garanties appropriées existent aux fins de la protection des données.

(151) Si un transfert n'est pas fondé sur un règlement d'adéquation ou des garanties appropriées, il ne peut avoir lieu que dans certaines circonstances bien précises, appelées «circonstances particulières»[215]. Tel est le cas lorsque le transfert est nécessaire: a) à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne; b) à la sauvegarde des intérêts légitimes de la personne concernée; c) à la prévention d'une menace grave et immédiate pour la sécurité publique d'un État membre ou d'un pays tiers; d) dans des cas particuliers, pour l'une des finalités répressives; ou e) dans des cas particuliers, à des fins juridiques (par exemple, dans le cadre d'une procédure judiciaire ou pour obtenir un avis juridique). Il est à noter que

213 L'article 2, paragraphe 2, de la loi de 1994 sur les services de renseignement dispose que «[l]e directeur du service de renseignement est responsable de l'efficacité de ce service et a le devoir de s'assurer — a) que des dispositions sont en vigueur afin de garantir qu'aucune information n'est obtenue par le service de renseignement, sauf si cela est nécessaire aux fins de l'exercice approprié de ses fonctions, et qu'aucune information n'est divulguée par celui-ci, sauf si cela est nécessaire — i) à cette fin; ii) aux fins de la sécurité nationale; iii) aux fins de la prévention ou de la détection des infractions graves; ou iv) aux fins de toute procédure pénale; et b) que le service de renseignement ne prend aucune mesure afin de servir les intérêts d'un parti politique du Royaume-Uni», tandis que l'article 2, paragraphe 2, de la loi de 1989 sur les services de sécurité prévoit que «[l]e directeur général est responsable de l'efficacité du service et il a le devoir de s'assurer a) que des dispositions sont en vigueur afin de garantir qu'aucune information n'est obtenue par le service, sauf si cela est nécessaire aux fins de l'exercice approprié de ses fonctions, et qu'aucune information n'est divulguée par celui-ci, sauf si cela est nécessaire à cette fin ou aux fins de la prévention ou de la détection] des infractions graves ou aux fins de toute procédure pénale]; b) que le service ne prend aucune mesure afin de servir les intérêts d'un parti politique; et c) que des dispositions ont été convenues avec le directeur général de l'agence nationale de lutte contre la criminalité afin de coordonner les activités du service, conformément à l'article 1er, paragraphe 4, de la présente loi, avec les activités des forces de police, de l'agence nationale de lutte contre la criminalité et des autres services répressifs».

214 Voir la partie 3, chapitre 5, de la DPA 2018.

215 Article 76 de la DPA 2018.

les points d) et e) ne s'appliquent pas si les droits et libertés de la personne concernée l'emportent sur l'intérêt public dans le cadre du transfert. Cet ensemble de circonstances correspond aux situations et aux conditions particulières qui sont considérées comme des «dérogations» au titre de l'article 38 de la directive (UE) 2016/680.

(152) De plus, lors de la remise à un pays tiers des éléments obtenus par des autorités répressives en vertu d'un mandat autorisant le recours à l'interception de communications ou à l'interférence avec des équipements, l'IPA 2016 impose des garanties supplémentaires. En particulier, une telle divulgation, définie comme une «divulgation à l'étranger», n'est autorisée que si l'autorité émettrice considère que des dispositions spécifiques appropriées sont en vigueur afin de limiter le nombre de personnes à qui les données sont divulguées, la mesure dans laquelle les éléments sont divulgués ou mis à disposition, ainsi que la mesure dans laquelle les éléments sont copiés et le nombre de copies réalisées. Par ailleurs, l'autorité émettrice peut considérer que des dispositions appropriées sont nécessaires pour garantir que toute copie d'une partie de ces éléments est détruite dès lors qu'il n'existe plus de motifs pertinents de la conserver (si elle n'a pas déjà été détruite)[216].

(153) Enfin, certains types de transferts ultérieurs du Royaume-Uni vers les États-Unis pourraient avoir lieu à l'avenir sur la base de l'accord entre le gouvernement du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord et le gouvernement des États-Unis d'Amérique relatif à l'accès aux données électroniques à des fins de lutte contre la grande criminalité (ci-après l'«accord Royaume-Uni/États-Unis» ou l'«accord»)[217], conclu en octobre 2019[218]. Bien que l'accord Royaume-Uni/États-Unis ne soit pas encore entré en vigueur au moment de l'adoption de la présente décision, son entrée en vigueur prochaine est susceptible d'avoir une incidence sur les transferts ultérieurs vers les États-Unis de données transférées en premier lieu vers le Royaume-Uni sur la base de la présente décision. Plus précisément, les données transférées depuis l'UE à des prestataires de services au Royaume-Uni pourraient faire l'objet d'injonctions de production de preuves électroniques émises par des autorités répressives américaines et rendues applicables au Royaume-Uni par cet accord, une fois celui-ci en vigueur.

---

216 Articles 54 et 130 de l'IPA 2016. Les autorités émettrices doivent examiner la nécessité d'imposer des garanties spécifiques concernant les éléments remis à des autorités étrangères, afin de s'assurer que les données font l'objet de garanties en matière de conservation, de destruction et de divulgation semblables à celles prévues aux articles 53 et 129 de l'IPA 2016.

217 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

218 Il s'agit d'un premier accord conclu en vertu de la loi américaine clarifiant l'utilisation légale des données à l'étranger (loi CLOUD). La loi CLOUD est une loi fédérale américaine adoptée le 23 mars 2018 qui précise, en modifiant la loi de 1986 sur la conservation des communications, que les fournisseurs de services américains sont tenus de se conformer aux injonctions de divulgation de données relatives ou non relatives au contenu émises par les autorités américaines, quel que soit le lieu de conservation de ces données. La loi CLOUD permet également la conclusion d'accords exécutifs avec des gouvernements étrangers, sur la base desquels les fournisseurs de services américains seraient en mesure de transmettre des données relatives au contenu directement à ces gouvernements étrangers (le texte de la loi CLOUD est disponible à l'adresse suivante: https://www.congress.gov/115/bills/s2383/BILLS-115s2383is.pdf).

C’est la raison pour laquelle l’évaluation des conditions dans lesquelles de telles injonctions peuvent être émises et exécutées, ainsi que des garanties applicables, est pertinente pour la présente décision.

(154) À cet égard, il convient de noter que premièrement, en ce qui concerne son champ d’application matériel, l’accord ne s’applique qu’aux infractions passibles d’une peine maximale d’au moins trois ans d’emprisonnement (définies comme des «infractions graves»)[219], y compris les «activités terroristes». Deuxièmement, les données traitées dans l’autre juridiction ne peuvent être obtenues au titre de cet accord qu’à la suite d’une «injonction […] sous réserve de l’examen ou du contrôle, en vertu du droit interne de la partie émettrice, d’une juridiction, d’un juge, d’un magistrat ou d’une autre autorité indépendante avant l’exécution de l’injonction, ou au cours d’une procédure y afférente»[220]. Troisièmement, toute injonction doit «être fondée sur l’exigence d’une justification raisonnable reposant sur des faits explicables et crédibles, ainsi que sur la particularité, la légalité et la gravité de la conduite faisant l’objet de l’enquête»[221] et «viser des comptes spécifiques, ainsi que désigner une personne, un compte, une adresse ou un équipement personnel en particulier, ou tout autre identifiant spécifique»[222]. Quatrièmement, les données obtenues au titre de cet accord bénéficient de protections équivalentes aux garanties spécifiques prévues par l’«accord-cadre UE-États-Unis»[223] – un accord global sur la protection des données conclu en décembre 2016 par l’Union et les États-Unis qui établit les garanties et les droits applicables aux transferts de données dans le domaine de la coopération des services répressifs – qui sont toutes intégrées dans cet accord par référence mutatis mutandis, notamment afin de tenir compte de la nature spécifique des transferts (à savoir des transferts d’opérateurs privés à une autorité répressive, et non des transferts entre autorités répressives)[224]. L’accord Royaume-Uni/États-Unis prévoit expressément que des protections équivalentes à celles prévues par l’accord-cadre UE-États-Unis s’appliqueront «à toutes les informations à caractère personnel produites dans le cadre de l’exécution d’injonctions au titre de l’accord, afin de fournir des protections équivalentes»[225].

(155) Les données transférées aux autorités américaines en vertu de l’accord Royaume-Uni/États-Unis devraient donc bénéficier des mêmes protections que celles prévues par un instrument du droit de l’Union, sous réserve des adaptations nécessaires en vue de refléter la nature des transferts en question. Les autorités britanniques ont par ailleurs confirmé que les protections prévues par l’accord-cadre s’appliqueront à l’ensemble des informations à caractère personnel produites ou conservées au titre de

---

219 Article 1er, paragraphe 14, de l’accord.

220 Article 5, paragraphe 2, de l’accord.

221 Article 5, paragraphe 1, de l’accord.

222 Article 4, paragraphe 5, de l’accord. Un autre critère plus strict s’applique en ce qui concerne l’interception de communications en temps réel: les injonctions doivent être émises pour une durée limitée, qui ne doit pas excéder la durée raisonnablement nécessaire à la réalisation des finalités de l’injonction, et uniquement si les mêmes informations ne pouvaient être raisonnablement obtenues au moyen d’une méthode moins intrusive (article 5, paragraphe 3, de l’accord).

223 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), disponible à l’adresse suivante: https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:22016A1210(01)&from=FR

224 Article 9, paragraphe 1, de l’accord.

225 Article 9, paragraphe 1, de l’accord.

l'accord, indépendamment de la nature ou du type d'organisme introduisant la demande (par exemple, les autorités répressives fédérales et des États aux États-Unis), afin qu'une protection équivalente soit prévue dans tous les cas. Toutefois, les autorités britanniques ont également expliqué que les détails de la mise en œuvre concrète des garanties en matière de protection des données font toujours l'objet de discussions entre le Royaume-Uni et les États-Unis. Dans le cadre des discussions avec les services de la Commission européenne sur la présente décision, les autorités britanniques ont confirmé qu'elles ne consentiraient à l'entrée en vigueur de l'accord qu'après s'être assurées que sa mise en œuvre est conforme aux obligations juridiques prévues par celui-ci et après avoir obtenu des éclaircissements en ce qui concerne le respect des normes en matière de protection des données pour toute donnée demandée au titre de cet accord. Dans la mesure où l'entrée en vigueur de l'accord est susceptible d'influer sur le niveau de protection évalué dans la présente décision, le Royaume-Uni est tenu de communiquer à la Commission européenne toute information et tout éclaircissement sur la manière dont les États-Unis respecteront les obligations leur incombant en vertu de l'accord, dès que cette information est disponible et, en tout état de cause, avant l'entrée en vigueur de l'accord, afin de garantir le suivi approprié de la présente décision conformément à l'article 45, paragraphe 4, du règlement (UE) 2016/679. Une attention particulière sera accordée à l'application et à l'adaptation des protections prévues par l'accord-cadre en fonction du type spécifique de transferts couverts par l'accord Royaume-Uni/États-Unis.

(156) De manière plus générale, toute évolution pertinente concernant l'entrée en vigueur et l'application de l'accord sera dûment prise en compte dans le cadre du suivi permanent de la présente décision, notamment s'agissant des conséquences nécessaires à tirer s'il y a la moindre indication qu'un niveau de protection essentiellement équivalent n'est plus assuré.

3.2.3 Surveillance

(157) 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 assurent la surveillance de l'utilisation de ces pouvoirs. Le commissaire à l'information surveille en particulier le traitement des données à caractère personnel lorsqu'il relève de la partie 3 de la DPA 2018[226]. Le Bureau du commissaire aux pouvoirs d'enquête (*Investigatory Powers Commissioner's Office*, IPCO) est responsable de la surveillance indépendante et judiciaire de l'utilisation des pouvoirs d'enquête au titre de l'IPA 2016[227] (les considérants (250) à (255) traitent de cette surveillance). De plus, le Parlement et d'autres organes assurent une surveillance supplémentaire.

3.2.3.1 Surveillance de la partie 3 de la DPA 2018

(158) Les fonctions générales du commissaire à l'information – dont l'indépendance et l'organisation sont décrites au considérant (87) – en ce qui concerne le traitement de données à caractère personnel relevant de la partie 3 de la DPA 2018 sont définies à l'annexe 13 de ladite loi. La mission principale de l'ICO consiste à surveiller et à faire appliquer la partie 3 de la DPA 2018, ainsi qu'à favoriser la sensibilisation du public et à conseiller le Parlement, le gouvernement et d'autres institutions et organes. Afin de

226 Article 116 de la DPA 2018.

227 Voir l'IPA 2016 et notamment son chapitre 1, partie 8.

préserver l'indépendance du pouvoir judiciaire, le commissaire à l'information n'est pas autorisé à exercer ses fonctions dans le cadre du traitement de données à caractère personnel par une personne physique ou une juridiction agissant dans l'exercice de sa fonction juridictionnelle. Dans un tel cas, d'autres organes exercent les fonctions de surveillance, comme l'expliquent les considérants (99) à (103).

(159) Le commissaire dispose de pouvoirs généraux d'enquête, de correction, d'autorisation et de conseil en lien avec le traitement de données à caractère personnel auquel s'applique la partie 3. En particulier, le commissaire dispose du pouvoir de notifier au responsable du traitement ou au sous-traitant une violation alléguée de la partie 3 de la DPA 2018, d'avertir ou de rappeler à l'ordre un responsable du traitement ou un sous-traitant qui a violé les dispositions de la partie 3 de cette loi, et d'émettre, de sa propre initiative ou sur demande, des avis à l'attention du Parlement, du gouvernement ou d'autres institutions et organismes ainsi que du public, sur toute question relative à la protection des données à caractère personnel[228].

(160) De plus, le commissaire dispose du pouvoir d'émettre des avis d'information[229], des avis d'évaluation[230] et des avis d'exécution[231], du pouvoir d'accéder aux documents et aux locaux[232] des responsables du traitement et des sous-traitants, ainsi que du pouvoir d'infliger des amendes administratives sous la forme d'avis de sanction[233]. La politique d'action réglementaire de l'ICO décrit les circonstances dans lesquelles il émet respectivement un avis d'information, d'évaluation, d'exécution ou de sanction[234] [voir également le considérant (93) et les considérants 101 et 102 de la décision d'adéquation en vertu de la directive (UE) 2016/680].

(161) Selon ses derniers rapports annuels (2018-2019[235], 2019-2020[236]), le commissaire à l'information a réalisé un certain nombre d'enquêtes et a pris des mesures d'exécution concernant le traitement de données par les autorités répressives. Le commissaire a, par exemple, mené une enquête et publié un avis en octobre 2019 concernant l'utilisation par les autorités répressives des technologies de reconnaissance faciale dans les lieux publics. L'enquête s'est notamment concentrée sur l'utilisation des capacités de reconnaissance faciale en direct par la South Wales Police et le Metropolitan Police Service (MPS). Le commissaire à l'information a également

228 Annexe 13, point 2, de la DPA 2018.

229 Ordonnant au responsable du traitement et au sous-traitant (et, dans certains cas, à toute autre personne) de communiquer les informations nécessaires (article 142 de la DPA 2018).

230 Permettant la réalisation d'enquêtes et d'audits, qui peuvent obliger le responsable du traitement ou le sous-traitant à autoriser le commissaire à pénétrer dans des locaux spécifiques, à inspecter ou à examiner des documents ou des équipements et à interroger les personnes chargées du traitement des données à caractère personnel pour le compte du responsable du traitement (article 146 de la DPA 2018).

231 Permettant l'exercice du pouvoir d'adopter des mesures correctrices, qui obligent les responsables du traitement/les sous-traitants à prendre ou à s'abstenir de prendre certaines mesures (article 149 de la DPA 2018).

232 Article 154 de la DPA 2018.

233 Article 155 de la DPA 2018.

234 Politique d'action réglementaire, voir la note de bas de page 96.

235 Rapport annuel et états financiers du commissaire à l'information pour la période 2018-2019, voir la note de bas de page 101.

236 Rapport annuel et états financiers du commissaire à l'information pour la période 2019-2020, voir la note de bas de page 82.

enquêté sur la «Gangs matrix»[237] du MPS et a constaté un ensemble de violations graves du droit relatif à la protection des données susceptibles de saper la confiance du public dans cette base de données et dans la manière dont les données étaient utilisées. En novembre 2018, le commissaire à l'information a émis un avis d'exécution et le MPS a ensuite adopté les mesures nécessaires afin de renforcer la sécurité et la responsabilité et de garantir une utilisation proportionnée des données. L'amende de 325 000 GBP infligée en mai 2018 par le commissaire au ministère public de la Couronne pour avoir perdu des DVD non chiffrés contenant des enregistrements d'interrogatoires de police constitue un autre exemple de mesure répressive dans ce domaine. Le commissaire à l'information a également enquêté sur des sujets plus généraux. Par exemple, au cours du premier semestre 2020, il s'est intéressé à l'extraction de données des téléphones portables à des fins policières et au traitement des données des victimes par la police. De plus, le commissaire enquête actuellement sur une affaire concernant l'accès des autorités répressives aux données détenues par une entité du secteur privé, Clearview AI Inc.[238]

(162) Outre les pouvoirs d'exécution du commissaire à l'information mentionnés aux considérants (160) et (161), certaines violations de la législation relative à la protection des données constituent des infractions et peuvent donc faire l'objet de sanctions pénales (article 196 de la DPA 2018). Ces infractions consistent, par exemple, à obtenir, à divulguer ou à conserver des données à caractère personnel sans le consentement du responsable du traitement et à obtenir la divulgation de données à caractère personnel à une autre personne sans le consentement du responsable du traitement[239], à réidentifier des informations qui constituent des données à caractère personnel anonymisées sans le consentement du responsable du traitement responsable de l'anonymisation de ces données[240], à empêcher, de manière intentionnelle, le commissaire d'exercer ses pouvoirs dans le cadre de l'inspection de données à caractère personnel conformément aux obligations internationales[241], à faire de fausses déclarations en réponse à un avis d'information, ou à détruire des informations en rapport avec des avis d'information et d'évaluation[242].

3.2.3.3 Autres organes de surveillance dans le domaine de l'application du droit pénal

(163) Outre le commissaire à l'information, il existe plusieurs autres organes de surveillance dans le domaine de l'application du droit pénal, qui disposent de mandats spécifiques concernant les questions de protection des données. Il s'agit par exemple du commissaire à la conservation et à l'utilisation de matériel biométrique (le

237 Une base de données dans laquelle étaient enregistrés des renseignements concernant des membres présumés de gangs et des victimes d'actes criminels liés aux gangs.

238 Voir la déclaration de l'ICO, disponible à l'adresse suivante: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/oaic-and-ico-open-joint-investigation-into-clearview-ai-inc/.

239 Article 170 de la DPA 2018.

240 Article 171 de la DPA 2018.

241 Article 119, paragraphe 6, de la DPA 2018.

242 Au cours de l'exercice financier couvrant la période allant du 1er avril 2019 au 31 mars 2020, les enquêtes de l'ICO ont donné lieu à des avertissements dans quatre cas et à des poursuites dans huit cas. Les poursuites ont été engagées au titre de l'article 55 de la DPA 1998, de l'article 77 de la loi de 2000 sur la liberté de l'information et de l'article 170 de la DPA 2018. Dans 75 % des cas, les mis en cause ont plaidé coupable, ce qui a évité de longs procès et les coûts correspondants. (Rapport annuel et états financiers du commissaire à l'information pour la période 2019-2020, voir la note de bas de page 87, page 40.)

«commissaire au matériel biométrique»)[243] et du commissaire aux caméras de surveillance[244].

3.2.3.4 Surveillance parlementaire dans le domaine de l'application du droit pénal

(164) La commission spéciale des affaires intérieures (*Home Affairs Select Committee*, HASC) assure la surveillance parlementaire dans le domaine de l'application du droit. Elle est composée de 11 parlementaires, issus des trois principaux partis politiques. Elle est chargée d'examiner les dépenses, la gestion et la politique du ministère de l'intérieur et des organes publics qui s'y rattachent, à savoir notamment la police et la NCA, dont les travaux peuvent faire l'objet d'une attention particulière de la part de la commission[245].

(165) La commission peut, dans la limite de ses compétences, choisir elle-même les sujets sur lesquels elle enquête, notamment des cas spécifiques, à condition que la justice n'en ait pas été saisie. La commission peut également chercher à obtenir des preuves écrites et orales auprès d'un large éventail de groupes et de personnes concernés. Elle produit des rapports sur ses constatations et formule des recommandations à

243 Le poste de commissaire au matériel biométrique a été créé par la loi de 2012 sur la protection des libertés (voir: https://www.legislation.gov.uk/ukpga/2012/9/contents). Les fonctions de ce commissaire sont, entre autres, de décider si la police peut ou non conserver les dossiers de profils ADN et les empreintes digitales des personnes qui ont été arrêtées mais ne sont pas accusées d'avoir commis une infraction désignée (article 63G de la loi PACE de 1984). En outre, le commissaire à la biométrie est investi d'une responsabilité générale consistant à surveiller la conservation et l'utilisation de l'ADN et des empreintes digitales, ainsi que la conservation pour des motifs de sécurité nationale (article 20, paragraphe 2, de la loi PoFA de 2012). Le commissaire à la biométrie est nommé en vertu du code de gouvernance sur les nominations publiques (disponible à l'adresse suivante: https://www.gov.uk/government/publications/governance-code-for-public-appointments) ses conditions d'engagement précisent clairement qu'il ne peut être démis de ses fonctions que par le ministre de l'intérieur et dans des circonstances strictement définies, dont le manquement à ses obligations professionnelles pour une durée de trois mois, une condamnation pour infraction pénale ou encore le non-respect de ses conditions d'engagement.

244 Le poste de commissaire aux caméras de surveillance a été créé par la loi de 2012 sur la protection des libertés. Le commissaire est chargé d'encourager le respect du code de bonnes pratiques relatif aux caméras de surveillance; d'examiner le fonctionnement de ce code et de fournir des conseils aux ministres concernant la nécessité de modifier ce code. Le commissaire est nommé en vertu des mêmes règles que le commissaire à la biométrie et jouit de pouvoirs, de ressources et d'une protection contre la révocation similaires.

245 Voir https://committees.parliament.uk/committee/83/home-affairs-committee/news/100537/work-of-the-national-crime-agency-scrutinised/

l'intention du gouvernement[246]. Le gouvernement doit répondre à chacune des recommandations des rapports, et ce dans un délai de 60 jours[247].

(166) Dans le domaine de la surveillance, la commission a publié un rapport concernant la loi de 2000 portant réglementation des pouvoirs d'enquête (RIPA 2000)[248], qui a conclu que cette loi n'était pas à même de remplir les objectifs fixés. Son rapport a été pris en compte lors du remplacement de plusieurs parties importantes de la RIPA 2000 par l'IPA 2016. Une liste complète des enquêtes est disponible sur le site internet de la commission[249].

(167) Les missions de la HASC sont exécutées par la sous-commission de la justice sur la police en Écosse et par la commission pour la justice en Irlande du Nord[250].

3.2.4 Recours

(168) En ce qui concerne le traitement de données par les autorités répressives, des mécanismes de recours sont 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.

(169) Cet ensemble de mécanismes donne aux personnes concernées des moyens de recours administratif et judiciaire efficaces, qui leur permettent notamment de protéger leurs droits, y compris le droit d'accéder aux données à caractère personnel les concernant ou d'obtenir la rectification ou l'effacement de telles données.

(170) Premièrement, conformément à l'article 165 de la DPA 2018, une personne concernée a le droit d'introduire une réclamation auprès du commissaire à l'information si elle considère qu'une violation de la partie 3 de la DPA 2018 a été commise en lien avec des données à caractère personnel la concernant[251]. Le commissaire à l'information a

246 Les commissions spéciales, notamment la commission spéciale des affaires intérieures, sont soumises au règlement intérieur de la Chambre des communes. Le règlement intérieur correspond aux règles fixées par la Chambre des communes qui régissent la manière dont le parlement fonctionne. Les commissions spéciales sont dotées de larges compétences, d'après l'article 152, paragraphe 1, du règlement intérieur, qui dispose que «[l]es commissions spéciales sont nommées pour examiner les dépenses, la gestion et la politique des principaux ministères, comme énoncé au paragraphe 2 de cet article, et des organismes publics qui s'y rattachent». Cela permet à la commission spéciale des affaires intérieures d'examiner toute politique relevant du ministère de l'intérieur, et notamment les politiques relatives aux pouvoirs d'enquête (et la législation correspondante). De plus, l'article 152, paragraphe 4, du règlement intérieur indique clairement que les commissions disposent de divers pouvoirs, dont celui de demander à des personnes de leur fournir des preuves ou des documents sur un sujet particulier et de publier des rapports. Les enquêtes en cours et passées de la commission sont disponibles à l'adresse suivante: https://committees.parliament.uk/committee/83/home-affairs-committee/.

247 Les pouvoirs de la commission spéciale des affaires intérieures en Angleterre et au pays de Galles sont définis dans le règlement intérieur de la Chambre des communes, disponible à l'adresse suivante: https://www.parliament.uk/business/publications/commons/standing-orders-public11/.

248 Consultable à l'adresse suivante: https://publications.parliament.uk/pa/cm201415/cmselect/cmhaff/711/71103.htm

249 Consultable à l'adresse suivante: https://committees.parliament.uk/committee/83/home-affairs-committee

250 Le règlement de la sous-commission de la justice sur la police en Écosse est disponible à l'adresse suivante: https://www.parliament.scot/parliamentarybusiness/CurrentCommittees/justice-committee.aspx et le règlement de la commission pour la justice en Irlande du Nord est disponible à l'adresse suivante: http://www.niassembly.gov.uk/assembly-business/standing-orders/]

251 Le dernier rapport annuel de l'ICO propose une ventilation de la nature des réclamations reçues et clôturées. Plus particulièrement, le nombre de réclamations reçues concernant «les opérations policières et le casier judiciaire» représentaient 6 % du nombre total de réclamations reçues (avec une hausse de 1 % par rapport à l'exercice financier précédent). Le rapport annuel montre également que les

le pouvoir d'évaluer le respect de la DPA 2018 par le responsable du traitement et le sous-traitant, de les obliger à prendre les mesures nécessaires en cas de non-respect et d'imposer des amendes.

(171) Deuxièmement, la DPA 2018 prévoit un droit de recours contre le commissaire à l'information si celui-ci ne traite pas de manière appropriée une réclamation introduite par la personne concernée. Plus précisément, si le commissaire ne «donne pas suite»[252] à une réclamation introduite par la personne concernée, l'auteur de la réclamation a le droit de former un recours juridictionnel puisqu'il peut demander à un tribunal de première instance[253] d'ordonner au commissaire de prendre les mesures appropriées pour donner suite à la réclamation ou pour informer l'auteur de la réclamation de l'état d'avancement de la réclamation[254]. En outre, toute personne à qui le commissaire adresse l'un des avis susmentionnés (avis d'information, d'évaluation, d'exécution ou de sanction) peut former un recours devant un tribunal de première instance. S'il considère que la décision du commissaire n'est pas conforme au droit ou que le commissaire à l'information aurait dû exercer son pouvoir discrétionnaire différemment, le tribunal doit faire droit au recours ou remplacer la décision du commissaire par un autre avis ou une autre décision que celui-ci aurait pu émettre ou prendre[255].

(172) Troisièmement, les personnes physiques peuvent former un recours juridictionnel contre les responsables du traitement et les sous-traitants directement devant les tribunaux. En particulier, en vertu de l'article 167 de la DPA 2018, une personne concernée peut introduire une demande auprès du tribunal concernant une violation de ses droits au titre de la législation relative à la protection des données et le tribunal peut, au moyen d'une ordonnance, demander au responsable du traitement de prendre (ou de s'abstenir de prendre) toute mesure en lien avec le traitement afin de respecter

---

réclamations concernant des demandes d'accès introduites par les personnes concernées étaient les plus nombreuses (46 % du nombre total de réclamations, avec une hausse de 8 % par rapport à l'exercice financier précédent) (rapport annuel de l'ICO pour la période 2019-2020, page 55; voir la note de bas de page 88).

252 L'article 166 de la DPA 2018 mentionne spécifiquement les situations suivantes: a) le commissaire ne prend pas les mesures appropriées pour donner suite à la réclamation, b) le commissaire n'informe pas l'auteur de la réclamation de l'état d'avancement ou de l'issue de la réclamation avant l'expiration du délai de trois mois à compter de la date de réception de la réclamation par le commissaire, ou c) si l'examen de la réclamation par le commissaire n'est pas mené à terme dans ce délai, le commissaire n'en informe pas l'auteur de la réclamation dans un nouveau délai de trois mois.

253 Le tribunal de première instance est le tribunal compétent pour juger des recours formés contre les décisions prises par les organismes de réglementation nationaux. En ce qui concerne les décisions du commissaire à l'information, la chambre compétente est la *General Regulatory Chamber*, dont la compétence s'exerce dans tout le Royaume-Uni.

254 Article 166 de la DPA 2018. Parmi les exemples de recours fructueux intentés contre l'ICO devant le tribunal figurent une affaire dans laquelle l'ICO avait accusé réception d'une réclamation introduite par une personne concernée mais n'avait pas indiqué la façon dont il comptait procéder et il lui a donc été ordonné de confirmer, dans un délai de 21 jours civils, s'il comptait enquêter sur la réclamation et, dans l'affirmative, d'informer l'auteur de la réclamation au moins tous les 21 jours civils de l'état d'avancement de l'enquête par la suite (le jugement n'a pas encore été publié) et une affaire dans laquelle le tribunal de première instance a considéré qu'il n'était pas possible d'établir clairement si la réponse de l'ICO à l'auteur d'une réclamation constituait bien l'«issue» de la réclamation (voir le jugement Susan Milne/The Information Commissioner [2020], disponible à l'adresse suivante: https://informationrights.decisions.tribunals.gov.uk/DBFiles/Decision/i2730/Milne,%20S%20-%20QJ2020-0296-GDPR-V,%20051220%20Section%20166%20DPA%20-DECISION.pdf).

255 Articles 162 et 163 de la DPA 2018.

la DPA 2018. De plus, en vertu de l'article 169 de la DPA 2018, toute personne ayant subi un préjudice du fait de la violation d'une des exigences de la législation relative à la protection des données (y compris de la partie 3 de la DPA 2018), autre que le RGPD britannique, a droit à une indemnisation au titre de ce préjudice par le responsable du traitement ou le sous-traitant, sauf si ceux-ci établissent qu'ils ne sont en aucun cas responsables de l'événement à l'origine de ce préjudice. Les préjudices incluent tant les pertes financières que les préjudices n'entraînant pas de perte financière, comme les situations de détresse.

(173) Enfin, toute personne, dans la mesure où elle estime que ses droits, notamment ses droits au respect de la vie privée et à la protection des données, ont été violés par une quelconque autorité publique, peut obtenir réparation devant les tribunaux du Royaume-Uni en vertu de la loi de 1998 sur les droits de l'homme[256]. Après avoir épuisé les voies de recours nationales, une personne physique, une organisation non gouvernementale ou un groupe de particuliers peut obtenir réparation auprès de la Cour européenne des droits de l'homme en cas de violation des droits garantis par la convention européenne des droits de l'homme[257] (voir le considérant (111)).

3.2.4.1 Mécanismes de recours possibles au titre de l'IPA 2016

(174) Les personnes physiques peuvent obtenir réparation en cas de violation de l'IPA 2016 auprès du tribunal chargé des pouvoirs d'enquête. Les voies de recours disponibles au titre de l'IPA 2016 sont décrites aux considérants (263) à (269) below ci-dessous.

3.3 Accès aux données et utilisation de celles-ci par les autorités publiques du Royaume-Uni à des fins de sécurité nationale

(175) Dans l'ordre juridique du Royaume-Uni, les services de renseignement habilités à collecter les informations électroniques détenues par les responsables du traitement ou les sous-traitants pour des motifs de sécurité nationale, dans des situations correspondant à un scénario d'adéquation, sont le *Security Service*[258] (MI5), le *Secret*

256 Voir, par exemple, l'affaire Brown/Commissioner of Police of the Metropolis & Anor [2019] EWCA Civ 1724, à l'issue de laquelle une indemnisation d'un montant de 9 000 GBP a été accordée au titre de la DPA 1998 et de la loi de 1998 sur les droits de l'homme en réparation de l'obtention illégale et de l'utilisation abusive d'informations à caractère personnel, et l'affaire R (on the application of Bridges)/Chief Constable of South Wales [2020] EWCA Civ 1058, dans laquelle la Cour d'appel a déclaré illégal le déploiement d'un système de reconnaissance faciale par la police du pays de Galles au motif que ce déploiement enfreignait l'article 8 de la CEDH et que l'analyse d'impact sur la protection des données produite par le responsable du traitement n'était pas conforme à la DPA 2018.

257 L'article 34 de la convention européenne des droits de l'homme prévoit que «[l]a Cour peut être saisie d'une requête par toute personne physique, toute organisation non gouvernementale ou tout groupe de particuliers qui se prétend victime d'une violation par l'une des Hautes Parties contractantes des droits reconnus dans la convention ou ses protocoles. Les Hautes Parties contractantes s'engagent à n'entraver par aucune mesure l'exercice efficace de ce droit».

258 Le MI5 est placé sous le contrôle du ministre de l'intérieur. La loi de 1989 sur les services de sécurité définit les fonctions du MI5: protéger la sécurité nationale (notamment contre les menaces émanant de l'espionnage, du terrorisme et du sabotage, des activités d'agents de puissances étrangères et des actions visant à renverser ou à affaiblir la démocratie parlementaire par des moyens politiques, industriels ou violents), sauvegarder la prospérité économique du Royaume-Uni face aux menaces extérieures et soutenir les activités des forces de police et d'autres services répressifs dans le cadre de la prévention et de la détection des infractions graves.

Intelligence Service[259] (SIS) et le *Government Communications Headquarters*[260] (GCHQ)[261].

3.3.1 Bases juridiques, limitations et garanties

(176) Au Royaume-Uni, les pouvoirs des agences de renseignement sont définis dans l'IPA 2016 et la RIPA 2000 qui, avec la DPA 2018, définissent le champ d'application matériel et personnel de ces pouvoirs ainsi que les limitations et garanties y afférentes. Ces pouvoirs, ainsi que les limitations et les garanties qui s'y appliquent, sont évalués en détail dans les sections suivantes.

3.3.1.1 Pouvoirs d'enquête exercés dans le cadre de la sécurité nationale

(177) L'IPA 2016 définit le cadre juridique relatif à l'utilisation des pouvoirs d'enquête, c.-à-d. le pouvoir d'intercepter les communications, d'accéder aux données de communication et d'interférer avec des équipements. L'IPA 2016 introduit une interdiction générale et constitue en infraction pénale le fait d'utiliser des techniques qui permettent d'accéder au contenu des communications, d'accéder aux données de communication ou d'interférer avec des équipements sans être légalement habilité à le faire[262]. C'est la raison pour laquelle l'utilisation de ces pouvoirs d'enquête n'est légale que lorsqu'elle s'effectue sur la base d'un mandat ou d'une autorisation[263].

(178) L'IPA 2016 fixe les règles détaillées régissant la portée et l'application de chacun des pouvoirs d'enquête, ainsi que leurs limitations et garanties spécifiques. Des règles différentes s'appliquent en fonction du type de pouvoir d'enquête (interception des

259 Le SIS est placé sous le contrôle du ministre des affaires étrangères et ses fonctions sont définies dans la loi de 1994 sur les services de renseignement. Elles consistent à obtenir et à fournir des informations concernant les actions ou les intentions de personnes situées en dehors des îles Britanniques et à accomplir d'autres missions ayant trait aux actions ou aux intentions de ces personnes. Ces fonctions ne peuvent être exercées que dans l'intérêt de la sécurité nationale, dans celui de la prospérité économique du Royaume-Uni ou aux fins de la prévention ou de la détection des infractions graves.

260 Le GCHQ est placé sous le contrôle du ministre des affaires étrangères et ses fonctions sont définies dans la loi de 1994 sur les services de renseignement. Elles consistent a) à surveiller, utiliser ou intercepter les émissions électromagnétiques et autres, ainsi que les équipements produisant de telles émissions, à obtenir et fournir des informations provenant de ces émissions, de ces équipements ou d'éléments chiffrés ou relatives à ceux-ci; b) à fournir des conseils et une assistance au niveau linguistique, notamment en ce qui concerne la terminologie utilisée à des fins techniques, la cryptographie et d'autres questions relatives à la protection des informations, aux forces armées, aux pouvoirs publics ou à d'autres organisations ou personnes considérées comme compétentes. Ces fonctions ne peuvent être exercées que dans l'intérêt de la sécurité nationale, dans celui de la prospérité économique du Royaume-Uni en lien avec les actions ou intentions de personnes situées en dehors des îles Britanniques ou aux fins de la prévention ou de la détection des infractions graves.

261 Le *Defence Intelligence* (DI), le *National Security Council and Secretariat*, la *Joint Intelligence Organisation* et le *Joint Intelligence Committee* sont d'autres organes publics qui exercent des fonctions importantes pour la sécurité nationale. Cependant, ni le JIC, ni la JIO ne sont en mesure de faire usage des pouvoirs d'enquête prévus par l'IPA 2016, tandis que le DI a des possibilités limitées d'utiliser ses pouvoirs.

262 Cette interdiction s'applique aux réseaux de communication tant privés que publics, ainsi qu'au service postal public lorsque l'interception est effectuée au Royaume-Uni. Elle ne s'applique pas au responsable du traitement du réseau privé si celui-ci a donné son consentement implicite ou explicite pour effectuer l'interception (partie 3 de l'IPA 2016).

263 Dans certains cas limités, il est possible d'effectuer une interception légale sans mandat, à savoir en cas d'interception avec le consentement de l'expéditeur ou du destinataire (article 44 de l'IPA 2016), dans le cas de finalités administratives ou répressives limitées (articles 45 à 48 de l'IPA 2016), dans certains établissements spécialisés (articles 49 à 51 de l'IPA 2016) et conformément à des demandes provenant de l'étranger (article 52 de l'IPA 2016).

communications, acquisition et conservation de données de communication et interférence avec des équipements)[264] et selon que le pouvoir soit exercé contre une cible spécifique ou en masse. Les détails concernant la portée, les garanties et les limitations de chaque mesure prévue par l'IPA 2016 sont décrits dans la partie consacrée à ce point ci-dessous.

(179) En outre, l'IPA 2016 est complétée par plusieurs codes de bonnes pratiques officiels publiés par le secrétaire d'État, approuvés par les deux chambres du Parlement[265] et applicables dans tout le pays, qui fournissent des orientations supplémentaires quant à l'utilisation de ces pouvoirs[266]. Alors que les personnes concernées peuvent directement s'appuyer sur les dispositions prévues par l'IPA 2016 pour exercer leurs droits, l'annexe 7, point 5, de l'IPA 2016 précise que les codes de bonnes pratiques peuvent être admis à titre de preuve dans le cadre de procédures civiles et pénales et que les juridictions ou les autorités de contrôle peuvent tenir compte de tout cas de non-respect des codes lorsqu'elles se prononcent sur une affaire dans le cadre d'une procédure judiciaire[267]. Dans le cadre de l'évaluation de la «qualité de la législation» et notamment de la précédente législation britannique dans le domaine de la surveillance, la RIPA 2000, la grande chambre de la Cour européenne des droits de l'homme a expressément reconnu la pertinence des codes de bonnes pratiques britanniques et admis que leurs dispositions pouvaient être prises en considération lors de l'examen de la prévisibilité de la législation autorisant la surveillance[268].

---

264 En ce qui concerne, par exemple, la portée de telles mesures, conformément à la partie 3 et à la partie 4 (conservation et acquisition de données de communication), la portée de la mesure est strictement liée à la définition des «opérateurs de télécommunications» dont les données des utilisateurs font l'objet de la mesure. On peut donner un autre exemple concernant l'utilisation des pouvoirs «de masse». Dans ce cas, la portée de ces pouvoirs est limitée aux « communications envoyées ou reçues par des personnes se trouvant en dehors des îles Britanniques».

265 L'annexe 7 de l'IPA 2016 définit la portée des codes, la procédure à suivre pour les publier, les règles applicables à leur révision et les effets qu'ils produisent.

266 Les codes de bonnes pratiques au titre de l'IPA 2016 sont disponibles à l'adresse suivante:https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice

267 Les juridictions utilisent les codes de bonnes pratiques pour évaluer la légalité de la conduite des autorités. Voir, par exemple, l'affaire Dias/Cleveland Police, [2017] UKIPTrib15_586-CH, dans laquelle le tribunal chargé des pouvoirs d'enquête a fait référence à des passages précis du code de bonnes pratiques relatif aux données de communication afin de comprendre la définition du motif «de prévention ou de détection d'une infraction ou de prévention des troubles à l'ordre public» utilisé pour justifier l'acquisition de données de communication. Le code a été inclus dans le raisonnement afin de déterminer si ce motif avait été invoqué à juste titre. Le tribunal a finalement conclu que les conduites contestées étaient illégales. Les tribunaux ont également évalué le niveau des garanties prévues par les codes, voir par exemple l'affaire Just for Law Kids/Secretary of State for the Home Department [2019] EWHC 1772 (Admin), dans laquelle la Haute Cour a conclu que la législation primaire et secondaire, ainsi que les orientations internes, apportaient des garanties suffisantes; ou l'affaire R (National Council for Civil Liberties)/Secretary of State for the Home Department & Others [2019] EWHC 2057 (Admin), dans laquelle il a été jugé que l'IPA 2016 et le code de bonnes pratiques relatif à l'interférence avec des équipements contenaient des dispositions suffisantes en ce qui concerne la nécessité de mandats spécifiques.

268 Dans l'arrêt Big Brother Watch, la grande chambre de la Cour européenne des droits de l'homme a noté que «[l]e code est un document public, approuvé par les deux chambres du Parlement, publié par le gouvernement en ligne et en version imprimée, et dont doivent tenir compte les personnes qui exercent des missions d'interception ainsi que les tribunaux (voir paragraphes 93 et 94 ci-dessus). En conséquence, la Cour a admis que ses dispositions pouvaient être prises en considération lors de l'examen de la prévisibilité de la RIPA (Kennedy, précité, § 157). En conséquence, la Cour accepterait que la législation locale soit "suffisamment accessible"». (Voir l'arrêt de la Cour européenne des droits

(180) Il convient alors de noter que les agences de sécurité nationale et certaines autorités répressives[269] disposent de pouvoirs ciblés (interception ciblée[270], acquisition de données de communication[271], conservation de données de communication[272] et interférence ciblée avec des équipements[273]), tandis que seuls les services de renseignement peuvent utiliser les pouvoirs de masse (c.-à-d. interception de masse[274], acquisition de masse de données de communication[275], interférence de masse avec des équipements[276] et ensembles de données à caractère personnel en masse[277]).

(181) Lorsqu'elle décide du pouvoir d'enquête à utiliser, l'agence de renseignement doit respecter les «obligations générales relatives à la protection de la vie privée» énumérées à l'article 2, paragraphe 2, point a), de l'IPA 2016, qui incluent un critère de nécessité et de proportionnalité. Plus précisément, conformément à cette disposition, une autorité publique qui a l'intention d'utiliser un pouvoir d'enquête doit prendre en compte i) la question de savoir si l'objectif visé par le mandat, l'autorisation ou l'avis pourrait être raisonnablement atteint par d'autres moyens moins intrusifs; ii) la question de savoir si le niveau de protection à appliquer 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 des informations en question, iii) l'intérêt public à assurer l'intégrité et la sécurité des systèmes de télécommunication et des services postaux et iv) tout autre aspect de l'intérêt public à assurer la protection de la vie privée[278].

(182) Les codes de bonnes pratiques applicables décrivent plus en détail la manière dont ces critères doivent être appliqués et la manière dont leur respect est évalué dans le cadre de l'autorisation d'utilisation de ces pouvoirs délivrée par le secrétaire d'État et les commissaires judiciaires indépendants. En particulier, le recours à l'un quelconque de ces pouvoirs d'enquête doit toujours être «proportionné à l'objectif visé, [ce qui] implique de mettre en balance la gravité de l'intrusion dans la vie privée (et les autres considérations mentionnées à l'article 2, paragraphe 2) avec la nécessité de l'activité

---

de l'homme (grande chambre) dans l'affaire Big Brother Watch et autres/Royaume-Uni, requêtes n° 58170/13, n° 62322/14 et n° 24960/15 du 25 mai 2021, paragraphe 366).

269 Pour la liste des autorités répressives compétentes qui peuvent faire usage de pouvoirs d'enquête ciblés au titre de l'IPA 2016, voir la note de bas de page (139).

270 Partie 2 de l'IPA 2016.

271 Partie 3 de l'IPA 2016.

272 Partie 4 de l'IPA 2016.

273 Partie 5 de l'IPA 2016.

274 Article 136 de l'IPA 2016.

275 Article 158 de l'IPA 2016.

276 Article 176 de l'IPA 2016.

277 Article 199 de l'IPA 2016.

278 Le code de bonnes pratiques relatif à l'interception des communications précise que les autres éléments du critère de proportionnalité sont les suivants: «i) la portée de l'ingérence envisagée dans la vie privée par rapport à l'objectif visé; ii) comment et pourquoi les méthodes à adopter provoqueront le moins d'interférences possible pour la personne et les tiers; iii) si l'activité constitue une utilisation appropriée de la loi ainsi qu'une manière raisonnable, après avoir envisagé toutes les autres solutions raisonnables, d'atteindre l'objectif visé; iv) quelles autres méthodes, le cas échéant, n'ont pas été mises en œuvre ou ont été employées mais ont été considérées comme insuffisantes pour atteindre les objectifs opérationnels sans recourir au pouvoir d'enquête envisagé». Point 4.16 du code de bonnes pratiques relatif à l'interception des communications, disponible à l'adresse suivante: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

du point de vue de l'enquête, des besoins opérationnels ou des capacités». Cela signifie notamment que l'utilisation de ces pouvoirs «devrait offrir une perspective réaliste d'apporter les avantages escomptés et ne devrait être ni disproportionnée, ni arbitraire» et qu'«[a]ucune ingérence dans la vie privée ne devrait être considérée comme proportionnée si les informations recherchées peuvent être raisonnablement obtenues par d'autres moyens moins intrusifs»[279]. Plus précisément, le respect du principe de proportionnalité doit être apprécié au regard des critères suivants: «i) la portée de l'ingérence envisagée dans la vie privée par rapport à l'objectif visé; ii) comment et pourquoi les méthodes à adopter provoqueront le moins d'interférences possible pour la personne et les tiers; iii) si l'activité constitue une utilisation appropriée de la loi ainsi qu'une manière raisonnable, après avoir envisagé toutes les autres solutions raisonnables, d'atteindre l'objectif visé; iv) quelles autres méthodes, le cas échéant, n'ont pas été mises en œuvre ou ont été employées mais ont été considérées comme insuffisantes pour atteindre les objectifs opérationnels sans recourir au pouvoir d'enquête envisagé»[280].

(183) En pratique, comme l'ont expliqué les autorités britanniques, cela permet de garantir qu'une agence de renseignement définit d'abord l'objectif opérationnel (et délimite ainsi la collecte, par ex. un objectif de lutte contre le terrorisme international dans une zone géographique donnée) puis, sur la base de cet objectif opérationnel, réfléchit à l'option technique (par ex. interception, interférence avec des équipements, acquisition de données de communication, ciblées ou de masse) la plus proportionnée (c.-à-d. la moins intrusive pour la vie privée, voir l'article 2, paragraphe 2, de l'IPA) à l'objectif visé et qui pourra donc être autorisée en vertu de l'une des bases législatives disponibles.

(184) Il convient de relever que le rapporteur spécial de l'ONU sur le droit à la vie privée, Joseph Cannataci, a également noté et salué ce recours à un critère de nécessité et de proportionnalité et a déclaré, en ce qui concerne le système institué par l'IPA 2016, que «[l]es procédures en place, au sein tant des services de renseignement que des autorités répressives, semblent systématiquement exiger de prendre en compte la nécessité et la proportionnalité d'une mesure ou d'une opération de surveillance avant que son autorisation soit recommandée, et de l'examiner sur les mêmes bases»[281]. Il a également fait observer que, lors de sa rencontre avec les représentants des autorités répressives et des agences de sécurité nationale, «[il a] observé un consensus sur le fait que le droit au respect de la vie privée doit être une considération prépondérante pour toute décision concernant les mesures de surveillance. Chacun a compris et apprécié l'importance de la nécessité et de la proportionnalité en tant que principes essentiels à prendre en compte».

(185) Les considérants (186) à (243) détaillent les critères spécifiques relatifs à la délivrance des différents mandats, ainsi que les limitations et les garanties établies par l'IPA 2016 concernant chaque pouvoir d'enquête.

---

279 Voir les points 4.12 et 4.15 du code de bonnes pratiques relatif à l'interception des communications, disponible à l'adresse suivante: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

280 Voir le point 4.16 du code de bonnes pratiques relatif à l'interception des communications.

281 Déclaration de fin de mission du rapporteur spécial sur le droit à la vie privée à l'issue de sa mission au Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, disponible à l'adresse suivante: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E, point 1.a.

3.3.1.1.1 Interception et examen ciblés

(186) On recense trois types de mandats permettant l'interception ciblée: le mandat d'interception ciblée[282], le mandat d'examen ciblé et un mandat d'entraide judiciaire[283]. La partie 2, chapitre 1, de l'IPA 2016 définit les conditions pour les obtenir, ainsi que les garanties applicables.

(187) Un mandat d'interception ciblée autorise l'interception des communications décrites dans celui-ci dans le cadre de leur transmission et l'obtention d'autres données utiles concernant ces communications[284], notamment des données secondaires[285]. Un mandat d'examen ciblé autorise une personne à procéder à la sélection des contenus obtenus dans le cadre d'un mandat d'interception de masse en vue de leur examen[286].

(188) Tout mandat au titre de la partie 2 de l'IPA 2016 peut être délivré par le secrétaire d'État[287] et approuvé par un commissaire judiciaire[288]. En tout état de cause, la durée de tout type de mandat ciblé est limitée à 6 mois[289] et des règles spécifiques s'appliquent à sa modification[290] et à son renouvellement[291].

(189) Avant de délivrer le mandat, le secrétaire d'État doit apprécier les principes de nécessité et de proportionnalité[292]. Plus précisément, avant de délivrer un mandat d'interception ciblée et un mandat d'examen ciblé, le secrétaire d'État doit vérifier si la mesure est nécessaire pour l'un des motifs suivants: l'intérêt de la sécurité nationale; la prévention ou la détection d'une infraction grave; ou les intérêts de la prospérité économique du Royaume-Uni[293], dans la mesure où ces intérêts relèvent aussi de la

---

282 Article 15, paragraphe 2, de l'IPA 2016.

283 Article 15, paragraphe 4, de l'IPA 2016.

284 Article 15, paragraphe 2, de l'IPA 2016.

285 Les données secondaires sont des données jointes ou logiquement associées à la communication interceptée qui peuvent être logiquement séparées de celle-ci et qui, si elles l'étaient, ne révéleraient rien de ce qui pourrait être raisonnablement considéré comme la signification (le cas échéant) de la communication. Les données secondaires peuvent par exemple correspondre aux configurations de routeurs ou aux pare-feu, ou à la durée pendant laquelle un routeur a été actif sur un réseau, lorsque ces éléments font partie de la communication interceptée, y sont joints ou y sont logiquement associés. Pour de plus amples informations, voir la définition contenue à l'article 16 de l'IPA 2016 et au point 2.19 du code de bonnes pratiques relatif à l'interception des communications, voir la note de bas de page 278.

286 Un tel examen est réalisé à titre d'exception à l'article 152, paragraphe 4, de l'IPA 2016, qui interdit de chercher à identifier les communications des particuliers qui se trouvent dans les îles Britanniques. Voir le considérant (229).

287 Le ministre écossais autorise le mandat lorsqu'il porte sur une activité criminelle grave en Écosse (voir les articles 21 et 22 de l'IPA 2016), tandis que le secrétaire d'État peut désigner un haut fonctionnaire pour délivrer un mandat d'entraide judiciaire lorsqu'il s'avère que l'interception concernera une personne ou des locaux situés en dehors du Royaume-Uni (article 40 de l'IPA 2016).

288 Articles 19 et 23 de l'IPA 2016.

289 Article 32 de l'IPA 2016.

290 Article 39 de l'IPA 2016. Des modifications limitées peuvent être apportées aux mandats par des personnes désignées, selon les conditions définies dans l'IPA 2016. La personne qui a délivré un mandat peut l'annuler à tout moment. Une telle annulation est obligatoire si le mandat n'est plus nécessaire pour aucun des motifs prévus ou si la conduite autorisée par le mandat n'est plus proportionnée à l'objectif visé.

291 Article 33 de l'IPA 2016. La décision de renouvellement du mandat doit être approuvée par un commissaire judiciaire.

292 Article 19 de l'IPA 2016.

293 Pour ce qui est de la notion d'«intérêts de la prospérité économique du Royaume-Uni, dans la mesure où ces intérêts relèvent aussi de la sécurité nationale», la grande chambre de la Cour européenne des

sécurité nationale[294]. Par ailleurs, un mandat d'entraide judiciaire (voir le considérant (139) above ci-dessus) ne peut être délivré que si le secrétaire d'État considère qu'il existe des circonstances équivalentes à celles dans lesquelles il aurait délivré un mandat aux fins de la prévention ou de la détection d'infractions graves[295].

(190) De plus, le secrétaire d'État doit évaluer si la mesure est proportionnée à l'objectif visé[296]. L'évaluation de la proportionnalité des mesures demandées doit tenir compte des obligations générales relatives à la protection de la vie privée énoncées à l'article 2, paragraphe 2, de l'IPA 2016, notamment de la nécessité d'apprécier si l'objectif visé par le mandat, l'autorisation ou l'avis pourrait être raisonnablement atteint par d'autres moyens moins intrusifs et si le niveau de protection à appliquer concernant l'obtention d'informations en vertu du mandat est plus élevé en raison de la nature particulièrement sensible des informations en question (voir le considérant (181) above ci-dessus).

(191) À cet effet, le secrétaire d'État devra tenir compte de tous les éléments de la demande introduite par l'autorité demandeuse, notamment de ceux qui concernent les personnes visées par l'interception et la pertinence de la mesure pour l'enquête. Ces éléments sont prévus par le code de bonnes pratiques relatif à l'interception des communications et doivent être décrits à un certain niveau de spécificité[297]. De plus, en vertu de l'article 17 de l'IPA 2016, tout mandat délivré en vertu du chapitre 2 de ladite loi doit nommer ou décrire la personne spécifique ou le groupe de personnes, l'organisation ou les locaux visés par l'interception (la «cible»). Dans le cas d'un mandat d'interception ciblée ou d'un mandat d'examen ciblé, il peut également s'agir d'un groupe de personnes, de plusieurs personnes ou organisations ou de plusieurs ensembles de locaux (également appelé «mandat thématique»)[298]. Dans ces cas, le mandat doit décrire l'objectif commun ou l'activité commune du groupe de personnes ou de l'opération/l'enquête et nommer ou décrire autant de personnes/d'organisations ou d'ensembles de locaux qu'il est raisonnablement possible de le faire[299]. Enfin, tous les mandats délivrés en vertu de la partie 2 de l'IPA 2016 doivent préciser les adresses, les numéros, les appareils, les facteurs ou la combinaison de facteurs devant être utilisés aux fins de l'identification des communications[300]. À cet égard, le code de bonnes pratiques relatif à l'interception des communications précise que, dans le cas d'un

---

droits de l'homme a estimé dans l'affaire Big Brother Watch et autres/Royaume-Uni (voir la note de bas de page 268 ci-dessus), point 371, que cette notion était suffisamment axée sur la sécurité nationale. Si la conclusion de la Cour dans cette affaire portait sur l'utilisation de cette notion dans la RIPA 2000, cette même notion est également utilisée dans l'IPA 2016.

294 Article 20, paragraphe 2, de l'IPA 2016.

295 Article 20, paragraphe 3, de l'IPA 2016.

296 Article 19, paragraphe 1, point b), article 19, paragraphe 2, point b), et article 19, paragraphe 3, point b), de l'IPA 2016.

297 Les informations demandées doivent notamment indiquer le contexte (description des personnes/organisations/ensembles de locaux, de la communication devant être interceptée) et dans quelle mesure l'obtention de ces informations profitera à l'enquête, ainsi que décrire la conduite devant être autorisée. Lorsqu'il n'est pas possible de décrire les personnes/l'organisation/les locaux, il convient d'expliquer pourquoi cette description n'était pas possible ou pourquoi seule une description générale a été faite (code de bonnes pratiques relatif à l'interception des communications, points 5.32 et 5.34, voir la note de bas de page 278).

298 Article 17, paragraphe 2, de l'IPA 2016. Voir également les points 5.11 et suivants du code de bonnes pratiques relatif à l'interception des communications, voir la note de bas de page 278.

299 Article 31, paragraphes 4 et 5, de l'IPA 2016.

300 Article 31, paragraphe 8, de l'IPA 2016.

mandat d'interception ciblée et d'un mandat d'examen ciblé, «le mandat doit préciser (ou décrire) les facteurs ou la combinaison de facteurs devant être utilisés aux fins de l'identification des communications. Lorsque les communications doivent être identifiées par référence à un numéro de téléphone (par exemple), le numéro doit être précisé et inscrit dans sa totalité. Toutefois, lorsque des sélecteurs internet très complexes ou changeant constamment doivent être utilisés pour identifier les communications, il convient de décrire ces sélecteurs dans la mesure du possible»[301].

(192) Dans ce contexte, le fait que l'évaluation effectuée par le secrétaire d'État en vue de délivrer un mandat doive être approuvée par un commissaire judiciaire indépendant[302], qui vérifiera notamment si la décision de délivrer le mandat respecte les principes de nécessité et de proportionnalité[303], constitue une garantie importante (au sujet du statut et du rôle des commissaires judiciaires, voir les considérants (251) à (256) below ci-dessous). L'IPA 2016 précise également que, lorsqu'il réalise une telle vérification, le commissaire judiciaire doit appliquer les mêmes principes que le ferait un tribunal pour une demande de contrôle juridictionnel[304]. Cela permet de garantir que dans chaque cas, et avant que l'accès aux données ne se fasse, un organe indépendant s'assure systématiquement du respect des principes de nécessité et de proportionnalité.

(193) L'IPA 2016 prévoit quelques exceptions particulières et limitées dans lesquelles il peut être procédé à une interception ciblée sans mandat. Ces cas limités sont précisés dans la loi[305] et, à l'exception du cas basé sur le «consentement» de l'expéditeur/du destinataire, les interceptions sont effectuées par des personnes (organismes privés ou publics) différentes des agences de sécurité nationale. Ce genre d'interceptions, qui plus est, sont réalisées à des fins autres que la collecte de «renseignements»[306] et, pour certaines d'entre elles, il est fortement improbable que cette collecte puisse avoir lieu dans le cadre d'un scénario de «transfert» (par exemple en cas d'interception effectuée dans un hôpital psychiatrique ou dans une prison). Compte tenu de la nature de l'organisme auquel s'appliquent ces cas particuliers (différent des agences de sécurité nationale), toutes les garanties prévues par la partie 2 de la DPA 2018 et par le RGPD britannique s'appliqueront, notamment la supervision de l'ICO et les mécanismes de recours disponibles. De surcroît, outre les garanties prévues par la DPA 2018, l'IPA 2016 prévoit aussi dans certains cas une surveillance ex post par l'IPCO[307].

(194) Lorsque l'interception est effectuée, des limitations et des garanties supplémentaires sont applicables en fonction du statut spécifique de la ou des personnes visées par

---

301 Points 5.37 et 5.38 du code de bonnes pratiques relatif à l'interception des communications, voir la note de bas de page 278.

302 L'approbation par un commissaire judiciaire n'est pas nécessaire lorsque le secrétaire d'État considère qu'il est urgent de délivrer le mandat (article 19, paragraphe 1, de l'IPA). Cependant, le commissaire judiciaire doit être informé dans les plus brefs délais et doit décider d'approuver ou non le mandat. S'il ne l'approuve pas, le mandat cesse de produire ses effets (articles 24 et 25 de l'IPA 2016).

303 Article 23, paragraphe 1, de l'IPA 2016.

304 Article 23, paragraphe 2, de l'IPA 2016.

305 Voir les articles 44 à 51 de l'IPA 2016 et l'article 12 du code de bonnes pratiques relatif à l'interception des communications (voir la note de bas de page 278).

306 C'est notamment le cas lorsqu'une interception est nécessaire en prison ou dans un hôpital psychiatrique (pour contrôler la conduite d'un détenu ou d'un patient) ou par un opérateur postal ou de télécommunication, afin, par exemple, de détecter des contenus abusifs.

307 Voir *a contrario* l'article 229, paragraphe 4, de l'IPA.

l'interception[308]. Par exemple, l'interception d'éléments couverts par le secret professionnel n'est autorisée qu'en présence de circonstances exceptionnelles et impérieuses; la personne délivrant le mandat doit tenir compte de l'intérêt public à assurer la confidentialité des éléments couverts par le secret professionnel et doit veiller à ce que des exigences spécifiques soient en place pour le traitement, la conservation et la divulgation de ces éléments[309].

(195) De plus, l'IPA 2016 prévoit des garanties spécifiques concernant la sécurité, la conservation et la divulgation, dont le secrétaire d'État devrait tenir compte avant de délivrer un mandat ciblé[310]. L'article 53, paragraphe 5, de l'IPA 2016 exige notamment que toute copie faite des éléments collectés en vertu du mandat soit conservée de manière sécurisée et soit détruite dès qu'il n'existe plus de motifs pertinents de la conserver, tandis que le paragraphe 2 dudit article exige que le nombre de personnes à qui les éléments sont divulgués et la mesure dans laquelle ces éléments sont divulgués, mis à disposition ou copiés soient limités au minimum nécessaire aux fins prévues par la loi.

(196) Enfin, lorsque les éléments qui ont été interceptés dans le cadre d'un mandat d'interception ciblée ou d'un mandat d'entraide judiciaire doivent être remis à un pays tiers («divulgation à l'étranger»), l'IPA 2016 impose au secrétaire d'État de veiller à ce que des dispositions appropriées soient en vigueur afin d'assurer que des garanties similaires en matière de sécurité, de conservation et de divulgation existent dans le pays en question[311]. En outre, l'article 109, paragraphe 2, de la DPA 2018 dispose que les services de renseignement ne peuvent transférer des données à caractère personnel en dehors du Royaume-Uni que si ce transfert est nécessaire et proportionné aux fins de l'exercice des fonctions réglementaires du responsable du traitement ou aux autres fins prévues par l'article 2, paragraphe 2, point a), de la loi de 1989 sur les services de sécurité ou par l'article 2, paragraphe 2, point a), et par l'article 4, paragraphe 2, point a), de la loi de 1994 sur les services de renseignement[312]. Il est important de noter que ces exigences s'appliquent aussi lorsque l'exemption concernant la sécurité nationale, conformément à l'article 110 de la DPA 2018, est invoquée, l'article 110 de la DPA 2018 n'incluant pas l'article 109 de la DPA 2018 au nombre des dispositions

---

308 Les articles 26 à 29 de l'IPA 2016 introduisent des limitations à l'obtention de mandats d'interception et d'examen ciblés en lien avec l'interception de communications envoyées par ou destinées à un membre du Parlement (de l'une des chambres du Parlement britannique), l'interception d'éléments couverts par le secret professionnel et l'interception de communications qui, selon les autorités qui les interceptent, contiendront des éléments journalistiques confidentiels, ainsi que lorsque l'objectif du mandat est d'identifier ou de confirmer l'identité d'une source d'information journalistique.

309 Article 26 de l'IPA 2016.

310 Article 19, paragraphe 1, de l'IPA 2016.

311 Article 54 de l'IPA 2016. Les garanties relatives à la communication d'éléments à des autorités étrangères sont encore précisées dans les codes de bonnes pratiques: voir notamment les points 9.26 et suivants et 9.87 du code de bonnes pratiques relatif à l'interception des communications et les points 9.33 et suivants et 9.41 du code de bonnes pratiques relatif à l'interférence (voir la note de bas de page 278).

312 Ces finalités sont les suivantes: pour le MI5, la prévention ou la détection des infractions graves ou toute procédure pénale [article 2, paragraphe 2, point a), de la loi de 1989 sur les services de sécurité]; pour le SIS, les intérêts de la sécurité nationale, la prévention ou la détection des infractions graves ou toute procédure pénale [article 2, paragraphe 2, point a), de la loi de 1994 sur les services de renseignement]; et, pour le GCHQ, toute procédure pénale [article 4, paragraphe 2, point a), de la loi de 1994 sur les services de renseignement]. Voir aussi les notes explicatives à la DPA 2018, disponibles à l'adresse suivante: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

pouvant être écartées si une exemption à certaines dispositions est requise pour garantir la sécurité nationale.

(197) 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.

(198) Le terme «données de communication» recouvre le «qui», le «quand», le «où» et le «comment» d'une communication, mais pas son contenu, c.-à-d. ce qui a été dit ou écrit. À la différence de l'interception, l'acquisition et la conservation de données de communication n'ont pas pour objectif d'obtenir le contenu de la communication, mais plutôt des informations concernant par exemple l'abonné à un service téléphonique ou une facture détaillée. 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[313].

(199) Il convient de noter que, généralement, la conservation et l'acquisition de données de communication ne concerneront pas les données à caractère personnel de personnes concernées de l'Union européenne transférées vers le Royaume-Uni au titre de la présente décision. L'obligation de conserver ou de divulguer les données de communication au titre des parties 3 et 4 de l'IPA 2016 concerne les données collectées par des opérateurs de télécommunications au Royaume-Uni directement auprès des utilisateurs d'un service de télécommunications[314]. Généralement, ce type

313 Les données de communication sont définies à l'article 261, paragraphe 5, de l'IPA 2016. On distingue deux catégories de données de communication: les «données sur les événements» (toute donnée qui identifie ou décrit un événement, par référence ou non à sa localisation, dans un système de télécommunications ou au moyen de ce dernier, lorsque l'événement consiste en une activité spécifique réalisée par une ou plusieurs entités à un moment donné) et les «données sur les entités» [toute donnée qui a) porte sur i) une entité, ii) une association entre un service de télécommunications et une entité, ou iii) une association entre toute partie d'un système de télécommunications et une entité, b) inclut ou consiste en des données qui identifient ou décrivent l'entité (par référence ou non à sa localisation), et c) n'est pas une donnée sur les événements].

314 Cela découle de la définition des données de communication proposée à l'article 261, paragraphe 5, de l'IPA 2016, selon laquelle les données de communication sont détenues ou obtenues par un opérateur de télécommunications et soit portent sur l'utilisateur d'un service de télécommunications et sur la fourniture de ce service, soit sont comprises dans une communication, en font partie, y sont jointes ou logiquement associées (voir également le code de bonnes pratiques relatif aux données de communication, disponible à l'adresse suivante: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf, points 2.22 à 2.33). De plus, selon la définition d'un «opérateur de télécommunications» proposée à l'article 261, paragraphe 10, de l'IPA 2016, il doit s'agir d'une personne qui propose ou fournit un service de télécommunications à des personnes au Royaume-Uni ou qui contrôle ou fournit un système de télécommunications se trouvant au Royaume-Uni ou contrôlé depuis ce pays (entièrement ou en partie). Ces définitions indiquent clairement que les obligations au titre de l'IPA 2016 ne peuvent pas être imposées aux opérateurs de télécommunications dont les équipements ne se trouvent pas au Royaume-Uni ou ne sont pas contrôlés depuis ce pays ou qui ne proposent ou ne fournissent pas de services à des personnes au Royaume-Uni (voir également le code de bonnes pratiques relatif aux données de communication, point 2.1). Si des abonnés de l'Union

de traitement «en contact avec la clientèle» n'implique pas un transfert au titre de la présente décision, c.-à-d. un transfert d'un responsable du traitement/sous-traitant de l'Union à un responsable du traitement/sous-traitant au Royaume-Uni.

(200) Cependant, par souci d'exhaustivité, les conditions et garanties régissant ces régimes d'acquisition et de conservation sont analysées dans les considérants suivants.

(201) Il convient tout d'abord de noter que la conservation et l'acquisition ciblée de données de communication sont à la disposition tant des agences de sécurité nationale que de certaines autorités répressives[315]. Les conditions pour exiger la conservation et/ou l'acquisition de données de communication peuvent varier en fonction du motif pour lequel la mesure est demandée, à savoir des fins de sécurité nationale ou des fins répressives.

(202) En particulier, si le nouveau régime a introduit l'exigence générale d'une autorisation ex ante délivrée par un organisme indépendant qui s'appliquera dans tous les cas où les données de communication sont conservées et/ou acquises (soit à des fins répressives, soit à des fins de sécurité nationale), à la suite de l'arrêt Tele2/Watson rendu par la Cour de justice de l'Union européenne[316], des garanties spécifiques ont été introduites lorsque la mesure est demandée à des fins répressives. En particulier, lorsque la conservation ou l'acquisition de données de communication est demandée à des fins répressives, l'autorisation ex ante doit toujours être accordée par le commissaire aux pouvoirs d'enquête. Ce n'est pas toujours le cas lorsque la mesure est demandée à des fins de sécurité nationale, étant donné que, comme décrit ci-dessous, ce type de mesures peut être autorisé par différentes «personnes accordant l'autorisation». En outre, le nouveau régime a étendu aux «infractions graves» le seuil pour lequel la conservation et l'acquisition de données de communication peuvent être autorisées[317].

i) Autorisation pour l'obtention de données de communication

(203) Conformément à la partie 3 de l'IPA 2016, les autorités publiques compétentes sont autorisées à obtenir des données de communication auprès d'un opérateur de télécommunications ou de toute personne capable d'obtenir et de divulguer de telles données. L'autorisation ne peut pas permettre l'interception du contenu des communications[318] et cesse de produire ses effets après un délai d'un mois[319]; elle peut

---

(qu'ils se trouvent dans l'Union ou au Royaume-Uni) ont recours à des services au Royaume-Uni, toute donnée de communication en lien avec la fourniture de ce service sera collectée directement par le fournisseur de services au Royaume-Uni plutôt que de faire l'objet d'un transfert depuis l'Union.

315 Les autorités compétentes sont énumérées à l'annexe 4 de l'IPA 2016 et elles comprennent les forces de police, les services de renseignement, certains ministères et administrations publiques, l'Agence nationale de lutte contre la criminalité, l'administration fiscale et douanière du Royaume-Uni, l'autorité de la concurrence et des marchés, le commissaire à l'information, les services d'urgence (ambulances, pompiers et services de secours) et des autorités par exemple dans le domaine de la santé et de la sécurité alimentaire.

316 Arrêt dans les affaires jointes C-203/15 et C-698/15, Tele2/Watson, ECLI:EU:C:2016:970.

317 Voir la section 61.7 (b) pour l'acquisition de données de communication et la section 87.10A pour la conservation des données de communication.

318 Article 60A, paragraphe 6, de l'IPA 2016.

319 Ce délai est réduit à trois jours lorsque l'autorisation est accordée pour des raisons d'urgence (article 65, paragraphe 3A, de l'IPA 2016).

être renouvelée sous réserve de l'obtention d'une autorisation supplémentaire[320]. L'acquisition de données de communication nécessite une autorisation du commissaire indépendant aux pouvoirs d'enquête (*Investigatory Powers Commissioner*, IPC)[321] (au sujet du statut et des pouvoirs de l'IPC, voir les considérants (250) à (251) below ci-dessous). C'est toujours le cas lorsque l'acquisition de données de communication est demandée par une autorité répressive compétente. Cependant, conformément à l'article 61 de l'IPA 2016, lorsque les données sont acquises dans l'intérêt de la sécurité nationale ou de la prospérité économique du Royaume-Uni, dans la mesure où cet intérêt relève aussi de la sécurité nationale, ou lorsqu'une demande est introduite par un membre d'une agence de renseignement en vertu de l'article 61, paragraphe 7, point b)[322], l'acquisition peut être autorisée[323] soit par l'IPC, soit par un haut fonctionnaire désigné[324]. Le haut fonctionnaire désigné doit être indépendant vis-à-vis de l'enquête ou de l'opération concernée et doit avoir des connaissances pratiques sur les principes relatifs aux droits de l'homme et la législation en la matière, notamment en ce qui concerne la nécessité et la proportionnalité[325]. La décision prise par le haut fonctionnaire désigné est soumise à une surveillance ex post assurée par l'IPC (voir le considérant (254) below ci-dessous pour de plus amples informations concernant les fonctions de surveillance ex post de l'IPC).

(204) L'autorisation d'acquérir des données de communication est fondée sur une appréciation de la nécessité et de la proportionnalité de la mesure. Plus précisément, la nécessité de la mesure est appréciée à la lumière des motifs énumérés dans la législation[326]. Compte tenu de la nature ciblée de cette mesure, elle doit également être

320 Selon l'article 65 de l'IPA 2016, l'autorisation renouvelée durera un mois à compter de la date d'expiration de l'autorisation en cours. La personne qui a accordé l'autorisation peut l'annuler à tout moment si elle considère que les exigences ne sont plus remplies.

321 Article 60A, paragraphe 1, de l'IPA 2016. L'Office des autorisations portant sur les données de communication (*Office for Communications Data Authorisations*, OCDA) exerce cette fonction pour le compte de l'IPC (voir les codes de bonnes pratiques relatifs aux données de communication, point 5.6).

322 La demande au titre de l'article 61, paragraphe 7, point b), de l'IPA 2016 est soumise «à une finalité applicable en matière pénale», ce qui signifie, selon l'article 61, paragraphe 7A, de l'IPA 2016: «lorsque les données de communication sont entièrement ou en partie des données sur les événements, la prévention ou la détection d'infractions graves; dans tout autre cas, la prévention ou la détection d'infractions ou la prévention de troubles à l'ordre public».

323 Le code de bonnes pratiques relatif aux données de communication précise que «[l]orsqu'une demande portant sur la sécurité nationale pourrait être introduite soit au titre de l'article 60A, soit au titre de l'article 61, ce sont les autorités publiques concernées qui déterminent quel mode d'autorisation est le plus approprié dans chaque cas. Les autorités publiques qui souhaitent avoir recours au mode d'autorisation par le haut fonctionnaire désigné devraient disposer d'orientations claires sur les circonstances dans lesquelles ce mode d'autorisation est approprié» (point 5.19 du code de bonnes pratiques relatif aux données de communication, disponible à l'adresse suivante: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822817/Communications_Data_Code_of_Practice.pdf).

324 L'article 70, paragraphe 3, de l'IPA 2016 définit le concept de «haut fonctionnaire désigné», qui change en fonction de l'autorité publique compétente (comme le prévoit l'annexe 4 de l'IPA 2016).

325 De plus amples informations sur l'indépendance du haut fonctionnaire désigné figurent dans le (code de bonnes pratiques relatif aux données de communication, points 4.12-4.17, voir note de bas de page 323).

326 Les motifs sont les suivants: i) la sécurité nationale; ii) la prévention ou la détection d'infractions ou la prévention de troubles à l'ordre public (dans le cas de «données sur les événements», uniquement des infractions graves); iii) les intérêts de la prospérité économique du Royaume-Uni, dans la mesure où ces intérêts relèvent aussi de la sécurité nationale; iv) les intérêts de la sécurité publique; v) la prévention du décès, de blessures ou de tout préjudice pour la santé physique ou mentale d'une personne, ou

nécessaire à une enquête ou à une opération spécifique[327]. Le code de bonnes pratiques relatif aux données de communication prévoit d'autres exigences concernant l'appréciation de la nécessité des mesures[328]. Ce code prévoit notamment que la demande présentée par l'autorité requérante devrait définir au minimum trois éléments permettant de justifier la nécessité d'une telle requête: i) l'événement visé par l'enquête, comme une infraction ou la localisation d'une personne vulnérable portée disparue; ii) la personne dont on cherche à obtenir les données, comme un suspect, un témoin ou une personne portée disparue, et la manière dont elle est liée à l'événement; et iii) les données de communication recherchées, comme le numéro de téléphone ou l'adresse IP, et la manière dont ces données sont liées à la personne et à l'événement[329].

(205) De plus, l'acquisition de données de communication doit être proportionnée à l'objectif visé[330]. Le code de bonnes pratiques relatif aux données de communication précise que, lorsqu'elle réalise une telle appréciation, la personne accordant l'autorisation devrait mettre en balance «la portée de l'ingérence dans les libertés et droits de la personne avec l'avantage particulier pour l'enquête ou l'opération menée dans l'intérêt public par l'autorité publique compétente» et que, compte tenu de l'ensemble des considérations propres à chaque cas, «il est possible qu'une ingérence dans les droits d'une personne ne soit pas justifiée car l'atteinte aux droits d'une autre personne ou d'un autre groupe de personnes serait trop grave». De plus, afin d'apprécier spécifiquement la proportionnalité de la mesure, le code énumère un certain nombre d'éléments qui devraient être inclus dans la demande présentée par l'autorité requérante[331]. Il convient en outre d'accorder une attention particulière au type de données de communication (données «sur les entités» ou «sur les événements»[332]) qui doivent être acquises et de recourir de préférence à la catégorie de données la moins intrusive[333]. Le code de bonnes pratiques relatif aux données de

---

l'atténuation de toute blessure ou de tout préjudice pour la santé physique ou mentale d'une personne; vi) l'assistance apportée dans le cadre d'enquêtes sur des erreurs judiciaires présumées; ou vii) l'identification d'une personne décédée ou de toute personne qui n'est pas en mesure de s'identifier en raison de son état de santé (article 61, paragraphe 7, de l'IPA 2016).

327 Article 60A, paragraphe 1, point b), de l'IPA 2016.

328 Points 3.3 et suivants du code de bonnes pratiques relatif aux données de communication, voir la note de bas de page 323.

329 Point 3.13 du code de bonnes pratiques relatif aux données de communication, voir la note de bas de page 323.

330 Article 60, paragraphe 1, point c), de l'IPA 2016.

331 Ces informations à inclure doivent contenir: i) une description de la manière dont l'obtention des données profitera à l'enquête ou à l'opération; ii) une explication de la pertinence des périodes de temps demandées, en indiquant en quoi ces périodes sont proportionnées à l'événement visé par l'enquête; iii) une explication de la raison pour laquelle le niveau d'intrusion est justifié compte tenu de l'avantage que les données apporteront à l'enquête (il y a lieu à cet égard de déterminer si des mesures d'enquête moins intrusives pourraient être mises en œuvre pour atteindre l'objectif en question); iv) une prise en compte des droits de la personne (notamment de son droit au respect de la vie privée et, le cas échéant, de son droit à la liberté d'expression) et une mise en balance de ces droits avec l'avantage pour l'enquête; v) des informations détaillées sur une potentielle intrusion collatérale et sur l'incidence que peuvent avoir les périodes de temps demandées sur cette intrusion (points 3.22 à 3.26 du code de bonnes pratiques relatif aux données de communication, voir la note de bas de page 323).

332 Voir la note de bas de page 313.

333 Lorsque des données de communication plus intrusives sont recherchées (par exemple des données sur les événements), le code précise qu'il est plus approprié d'acquérir d'abord des données sur les entités ou d'acquérir directement des données sur les événements dans certains cas limités d'urgence

communication contient également des instructions spécifiques concernant les autorisations portant sur les données de communication de personnes exerçant des professions particulières (comme les médecins, les avocats, les journalistes, les parlementaires ou les ministres des cultes)[334], qui sont soumises à des garanties supplémentaires[335].

ii) Avis nécessitant la conservation des données de communication

(206) La partie 4 de l'IPA 2016 définit les règles applicables à la conservation des données de communication, et notamment les critères permettant au secrétaire d'État de délivrer un avis de conservation[336]. Les garanties prévues par l'IPA sont les mêmes lorsque les données sont conservées soit à des fins répressives, soit dans l'intérêt de la sécurité nationale.

(207) La délivrance de ces avis de conservation 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[337]. 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 et décrite aux considérants (203) à (205).

(208) L'exercice du pouvoir d'exiger la conservation de certaines données est soumis à un certain nombre de limitations et de garanties. Le secrétaire d'État ne peut délivrer d'avis de conservation à un ou plusieurs opérateurs[338] que lorsqu'il considère que l'obligation de conserver les données est nécessaire à l'une des finalités prévues par la loi[339] et qu'elle est proportionnée à l'objectif visé[340]. Comme le précise l'IPA 2016

---

particulière (points 6.10 à 6.14 du code de bonnes pratiques relatif aux données de communication, voir la note de bas de page 323).

334 Points 8.8 à 8.44 du code de bonnes pratiques relatif aux données de communication, voir la note de bas de page 323.

335 Le code de bonnes pratiques précise que «la personne accordant l'autorisation doit examiner ces demandes avec un soin particulier, et notamment prendre en compte les conséquences non souhaitées que ces demandes pourraient avoir et la question de savoir si ces demandes servent au mieux l'intérêt public» (point 8.8 du code de bonnes pratiques relatif aux données de communication). De plus, il convient de tenir un registre de ce type de demandes et, lors de la prochaine inspection, de les porter à l'attention de l'IPC (point 8.10 du code de bonnes pratiques relatif aux données de communication, voir la note de bas de page 323).

336 Articles 87 à 89 de l'IPA 2016.

337 Conformément à l'article 90 de l'IPA 2016, un opérateur de télécommunications à qui est remis un avis de conservation peut demander un réexamen au secrétaire d'État qui l'a délivré.

338 Conformément à l'article 87, paragraphe 2, point a), de l'IPA 2016, un avis de conservation peut se rapporter «à un opérateur en particulier ou à toute catégorie d'opérateurs».

339 Ces finalités sont les suivantes: i) les intérêts liés à la sécurité nationale; ii) la finalité applicable en matière pénale (comme le définit l'article 87.10A de l'IPA 2016); iii) les intérêts de la prospérité économique du Royaume-Uni, dans la mesure où ces intérêts relèvent aussi de la sécurité nationale; iv) les intérêts de la sécurité publique; v) la prévention du décès, de blessures ou de tout préjudice pour la santé physique ou mentale d'une personne, ou l'atténuation de toute blessure ou de tout préjudice pour la santé physique ou mentale d'une personne; ou vi) l'assistance apportée dans le cadre d'enquêtes sur des erreurs judiciaires présumées (article 87 de l'IPA 2016).

340 Article 87 de l'IPA 2016. De plus, conformément au code de bonnes pratiques applicable, afin d'apprécier la proportionnalité de l'avis de conservation, les critères prévus à l'article 2, paragraphe 2, de l'IPA 2016 s'appliquent, notamment l'obligation d'apprécier si l'objectif visé par l'avis pourrait être

elle-même[341], avant de délivrer un avis de conservation, le secrétaire d'État doit tenir compte: des avantages probables de l'avis[342]; d'une description des services de télécommunications; de l'opportunité de limiter les données à conserver par référence à leur localisation ou à une description des personnes auxquelles sont fournis les services de télécommunications[343]; du nombre probable d'utilisateurs (s'il est connu) de tout service de télécommunications sur lequel porte l'avis[344]; de la faisabilité technique du respect de l'avis; du coût probable engendré par le respect de l'avis et de tout autre effet que pourrait produire l'avis sur l'opérateur de télécommunications (ou la description des opérateurs) concerné[345]. Comme le décrit plus en détail le chapitre 17 du code de bonnes pratiques relatif aux données de communication, tous les avis de conservation doivent préciser chaque type de données à conserver, ainsi que la manière dont les types de données en question respectent le critère de nécessité de la conservation.

(209) Dans tous les cas (tant à des fins sécurité nationale qu'à des fins répressives), la décision du secrétaire d'État de délivrer l'avis de conservation doit être approuvée par un commissaire judiciaire indépendant, dans le cadre de la procédure dite «de double verrouillage», qui doit notamment vérifier si l'avis de conservation des données de communication pertinentes est nécessaire et proportionné pour l'une ou plusieurs des finalités prévues[346].

3.3.1.1.3 Interférence avec des équipements

(210) L'interférence avec des équipements est un ensemble de techniques utilisées afin d'obtenir diverses données à partir d'équipements[347] tels que les ordinateurs, les tablettes et les smartphones, ainsi que les câbles, les fils et les appareils de stockage[348].

---

raisonnablement atteint par des moyens moins intrusifs. Tout comme pour l'appréciation de la proportionnalité de l'acquisition des données de communication, le code de bonnes pratiques relatif aux données de communication précise qu'une telle appréciation nécessite «la mise en balance de la portée de l'ingérence dans le droit de la personne au respect de sa vie privée avec l'avantage particulier pour l'enquête menée» (point 16.3 du code de bonnes pratiques relatif aux données de communication, voir la note de bas de page 323).

341 Voir l'article 88 de l'IPA 2016.

342 Les avantages peuvent être existants ou prévus et doivent concerner les finalités prévues par la loi pour lesquelles les données peuvent être conservées (point 17.17 du code de bonnes pratiques relatif aux données de communication, voir la note de bas de page 323).

343 Ces considérations consisteront notamment à déterminer si la totalité de la portée géographique de l'avis de conservation est nécessaire et proportionnée et s'il est nécessaire et proportionné d'inclure ou d'exclure une description particulière des personnes (point 17.17 du code de bonnes pratiques relatif aux données de communication, voir la note de bas de page 323).

344 Cela aidera le secrétaire d'État à prendre en compte aussi bien le niveau d'intrusion pour les clients que les avantages probables des données devant être conservées (point 17.17 du code de bonnes pratiques relatif aux données de communication, voir la note de bas de page 323).

345 Article 88 de l'IPA 2016.

346 Article 89 de l'IPA 2016.

347 Conformément à l'article 135, paragraphe 1, et à l'article 198, paragraphe 1, de l'IPA 2016, le terme «équipements» recouvre les équipements produisant des émissions électromagnétiques, acoustiques ou autres et tout appareil pouvant être utilisé en lien avec ces équipements.

348 Code de bonnes pratiques relatif à l'interférence avec des équipements, disponible à l'adresse suivante: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf , point 2.2.

L'interférence avec des équipements permet d'obtenir à la fois le contenu des communications et des données relatives aux équipements[349].

(211) Conformément à l'article 13, paragraphe 1, de l'IPA 2016, le recours à l'interférence avec des équipements par les services de renseignement doit être autorisé au moyen d'un mandat suivant la procédure «de double verrouillage» établie par l'IPA 2016, à condition qu'il existe une «connexion avec les îles Britanniques»[350]. Selon les explications fournies par les autorités britanniques, dans le cas d'un transfert de données depuis l'Union européenne vers le Royaume-Uni au titre de la présente décision, il existerait toujours une «connexion avec les îles Britanniques» et toute interférence avec des équipements couvrant ces données serait donc soumise à l'obligation de mandat prévue par l'article 13, paragraphe 1, de l'IPA 2016[351].

(212) La partie 5 de l'IPA 2016 définit les règles applicables aux mandats d'interférence ciblée avec des équipements. À l'instar de l'interception ciblée, l'interférence ciblée avec des équipements doit concerner une «cible» particulière, qui doit être précisée dans le mandat[352]. Les détails sur la manière dont la «cible» doit être identifiée

---

349 Les données relatives aux équipements sont définies à l'article 100 de l'IPA 2016 comme des données relatives aux systèmes et des données a) qui sont comprises dans une communication ou un autre élément d'information, en font partie, y sont jointes ou logiquement associées (que ce soit le fait de l'expéditeur ou non); b) qui peuvent être logiquement séparées du reste de la communication ou de l'élément d'information et c) qui, si elles étaient séparées, ne révéleraient rien de ce qui pourrait être raisonnablement considéré comme la signification (le cas échéant) de la communication ou de l'élément d'information.

350 Pour qu'un mandat soit obligatoire, l'article 13, paragraphe 1, de l'IPA 2016 exige également que la conduite du service de renseignement constitue une ou plusieurs infractions au titre des articles 1 à 3A de la loi de 1990 sur l'utilisation abusive de l'informatique, ce qui serait le cas dans la plupart des circonstances, voir les points 3.32 et 3.6 à 3.9 du code de bonnes pratiques relatif à l'interférence avec des équipements. Conformément à l'article 13, paragraphe 2, de l'IPA 2016, il existe une «connexion avec les îles Britanniques» si a) une partie de la conduite a lieu dans les îles Britanniques (indépendamment de l'emplacement de l'équipement faisant ou pouvant faire l'objet d'une interférence), b) le service de renseignement considère qu'une partie de l'équipement faisant ou pouvant faire l'objet d'une interférence se trouve ou pourrait se trouver dans les îles Britanniques à un moment donné pendant que l'interférence a lieu, ou c) l'objectif de l'interférence est d'obtenir i) des communications envoyées par ou destinées à une personne qui se trouve, ou dont le service de renseignement pense qu'elle se trouve, à ce moment donné dans les îles Britanniques, ii) des informations privées concernant une personne qui se trouve, ou dont le service de renseignement pense qu'elle se trouve, à ce moment donné dans les îles Britanniques, ou iii) des données relatives aux équipements qui font partie de communications ou d'informations privées relevant du point i) ou ii) ou qui y sont liées.

351 Par souci d'exhaustivité, il convient de noter que même dans les cas où il n'existe pas de «connexion avec les îles Britanniques» et où le recours à l'interférence avec des équipements n'est donc pas soumis à l'obligation de mandat prévue par l'article 13, paragraphe 1, de l'IPA 2016, un service de renseignement qui prévoit de commencer une activité pour laquelle il est en mesure d'obtenir un mandat d'interférence de masse avec des équipements devrait par principe se procurer un tel mandat (voir le point 3.24 du code de bonnes pratiques relatif à l'interférence avec des équipements). Même lorsqu'un mandat d'interférence avec des équipements au titre de l'IPA 2016 n'est ni requis par la loi, ni obtenu par principe, les actions des services de renseignement sont soumises à un certain nombre de conditions et de limitations en vertu de l'article 7 de la loi de 1994 sur les services de renseignement. Parmi ces conditions figure l'obligation d'obtenir une autorisation du secrétaire d'État, qui doit s'assurer que toute action reste dans les limites de ce qui est nécessaire à la bonne exécution des missions du service de renseignement.

352 L'article 115 de l'IPA 2016 régit le contenu du mandat et précise qu'il doit inclure le nom ou la description des personnes, des organisations, du lieu ou du groupe de personnes qui constituent la «cible», une description de la nature de l'enquête et une description des activités pour lesquelles

dépendent de l'objet et du type d'équipements devant faire l'objet de l'interférence. Plus particulièrement, l'article 115, paragraphe 3, de l'IPA précise les éléments devant être inclus dans le mandat (par ex. le nom de la personne ou de l'organisation, une description de la localisation) selon si, par exemple, l'interférence concerne un équipement qui appartient à une personne, à une organisation ou à un groupe de personnes en particulier, est utilisé par ces derniers ou est en leur possession, ou se trouve dans un endroit spécifique, etc.[353] Les finalités pour lesquelles les mandats d'interférence ciblée avec des équipements peuvent être délivrés dépendent de l'autorité publique qui en fait la demande[354].

(213) De même que pour l'interception ciblée, l'autorité délivrant le mandat doit déterminer si la mesure est nécessaire pour atteindre un objectif spécifique et si elle est proportionnée à l'objectif visé[355]. De plus, elle doit également déterminer si des garanties existent en lien avec la sécurité, la conservation et la divulgation, ainsi qu'avec la «divulgation à l'étranger»[356] (voir le considérant (196) ci-dessus).

(214) Le mandat doit être approuvé par un commissaire judiciaire, sauf en cas d'urgence[357]. Dans ce cas, un commissaire judiciaire doit être informé de la délivrance d'un mandat et doit l'approuver dans un délai de trois jours ouvrables. Si le commissaire judiciaire refuse de l'approuver, le mandat cesse de produire ses effets et ne peut pas être renouvelé[358]. En outre, le commissaire judiciaire a le pouvoir d'exiger que toute donnée interceptée en vertu du mandat soit supprimée[359]. Le fait qu'un mandat ait été délivré en urgence n'a pas d'incidence sur la surveillance ex post (voir considérants (244) à (255)) ou sur les possibilités pour les particuliers de demander réparation (voir considérants (260) à (270)). Les particuliers peuvent introduire une plainte auprès de l'ICO ou introduire une réclamation contre tout comportement allégué devant le

---

l'équipement est utilisé. Il doit également décrire le type d'équipement et la conduite que la personne destinataire du mandat est autorisée à adopter.

353 Voir également le point 5.7 du code de bonnes pratiques relatif à l'interférence avec des équipements, voir la note de bas de page 348.

354 Les agences de sécurité nationale peuvent demander un mandat d'interférence avec des équipements lorsque cela est nécessaire à des fins de sécurité nationale, aux fins de la détection d'infractions graves et/ou dans l'intérêt de la prospérité économique du Royaume-Uni dans la mesure où cet intérêt relève aussi de la sécurité nationale (articles 102 et 103 de l'IPA 2016). En fonction de l'agence, un mandat d'interférence avec des équipements peut être requis à des fins répressives lorsqu'il est nécessaire à la détection ou à la prévention d'une infraction grave ou à la prévention du décès, de blessures ou de tout préjudice pour la santé physique ou mentale d'une personne, ou à l'atténuation de toute blessure ou de tout préjudice pour la santé physique ou mentale d'une personne (voir l'article 106, paragraphes 1 et 3, de l'IPA 2016).

355 Article 102, paragraphe 1, de l'IPA 2016.

356 Articles 129 à 131 de l'IPA 2016.

357 Article 109 de l'IPA 2016.

358 Article 109, paragraphe 4, de l'IPA 2016.

359 Article 110, paragraphe 3, point b), de l'IPA 2016. Conformément au point 5.67 du code de bonnes pratiques relatif à l'interférence avec des équipements, l'urgence est déterminée par la question de savoir s'il serait raisonnablement possible de demander l'approbation du commissaire judiciaire pour délivrer le mandat dans le délai disponible pour répondre à un besoin opérationnel ou d'enquête. Les mandats urgents devraient relever de l'une ou des deux catégories suivantes: i) une menace imminente pour la vie ou des atteintes graves - par exemple, si une personne a été enlevée et qu'il est estimé que sa vie est en danger imminent; ou ii) une possibilité de collecte de renseignements ou d'enquête assortie d'un délai limité pour agir - par exemple, un envoi de drogues de catégorie A est sur le point d'entrer au Royaume-Uni et les services répressifs veulent disposer d'une couverture des auteurs d'infractions graves afin de procéder à des arrestations. Voir la note de bas de page 348.

tribunal chargé des pouvoirs d'enquête selon la procédure habituelle. Dans tous les cas, le critère appliqué par le commissaire judiciaire pour décider d'approuver ou non le mandat est celui de la nécessité et de la proportionnalité tel qu'il s'applique aux demandes d'interception ciblée[360] (voir le considérant (192) aboveci-dessus).

(215) Enfin, les garanties spécifiques applicables à l'interception ciblée s'appliquent également à l'interférence avec des équipements en ce qui concerne la durée, le renouvellement et la modification du mandat, ainsi que l'interception de communications de parlementaires, d'éléments couverts par le secret professionnel et d'éléments journalistiques (pour de plus amples informations, voir le considérant 193 ci-dessus).

3.3.1.1.4 Exercice des pouvoirs de masse

(216) Les pouvoirs de masse sont régis par la partie 6 de l'IPA 2016. De plus, les codes de bonnes pratiques apportent des précisions sur l'utilisation de ces pouvoirs. Bien que le droit britannique ne donne aucune définition du terme «pouvoir de masse», dans le cadre de l'IPA 2016, ce terme a été décrit comme la collecte et la conservation d'une grande quantité de données acquises par le gouvernement par différents moyens (c.-à-d. les pouvoirs d'interception de masse, d'acquisition de masse et d'interférence de masse avec des équipements et ceux liés aux ensembles de données à caractère personnel en masse), auxquelles peuvent ensuite accéder les autorités. Cette description est précisée en l'opposant à ce que le terme «pouvoir de masse» ne recouvre pas: il ne s'agit pas d'une «surveillance de masse» sans limitation ni garantie. Bien au contraire, comme expliqué plus bas, il intègre des limitations et des garanties conçues pour faire en sorte que l'accès aux données ne soit pas accordé de manière indifférenciée ou injustifiée[361]. En particulier, les pouvoirs de masse ne peuvent être utilisés que si un lien est établi entre la mesure technique que souhaite mettre en œuvre une agence nationale de renseignement et l'objectif opérationnel pour lequel une telle mesure est demandée.

(217) De plus, seules les agences de renseignement disposent de pouvoirs de masse et ces derniers sont toujours soumis à un mandat délivré par le secrétaire d'État et approuvé par un commissaire judiciaire. Lors du choix de la méthode de collecte des renseignements, il convient de déterminer si l'objectif poursuivi peut être atteint par des «moyens moins intrusifs»[362]. Cette approche découle du cadre législatif qui est fondé sur le principe de proportionnalité et donne donc la priorité à la collecte ciblée par rapport à la collecte de masse.

---

360 Article 108 de l'IPA 2016.

361 Selon le rapport sur les pouvoirs de masse présenté par Lord David Anderson, contrôleur indépendant de la législation sur le terrorisme, en vue de l'approbation de l'IPA 2016, «*il convient d'établir clairement que la collecte et la conservation de données en masse ne constituent pas une "surveillance de masse". Tout système juridique digne de ce nom intégrera des limitations et des garanties conçues précisément pour garantir que l'accès à des banques de données sensibles […] n'est pas accordé de manière indifférenciée ou injustifiée. De telles limitations et garanties existent à l'évidence dans la proposition de loi*. Lord David Anderson, rapport sur l'examen des pouvoirs de masse, août 2016, point 1.9 (soulignement ajouté), disponible à l'adresse suivante: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546925/56730_Cm9326_WEB.PDF

362 Article 2.2 de l'IPA 2016. Voir par exemple le point 4.11 du code de bonnes pratiques relatif à l'acquisition de masse de données de communication, disponible à l'adresse suivante: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf

3.3.1.1.4.1 Interception de masse et interférence de masse avec des équipements

(218) Le régime applicable à l'interception de masse est prévu à la partie 6, chapitre 1 de l'IPA 2016, tandis que le chapitre 3 de ladite partie régit l'interférence de masse avec des équipements. Ces régimes étant en substance les mêmes, les conditions et les garanties supplémentaires applicables à ces mandats font l'objet d'une analyse conjointe.

i) Conditions et critères relatifs à la délivrance du mandat

(219) Un mandat d'interception de masse se limite à l'interception de communications dans le cadre de leur transmission, envoyées ou reçues par des personnes se trouvant en dehors des îles Britanniques[363], appelées «communications en lien avec l'étranger»[364], ainsi que d'autres données utiles et à la sélection ultérieure des éléments interceptés en vue de leur examen[365]. Un mandat d'interférence de masse avec des équipements[366] autorise son destinataire à procéder à des interférences avec tout équipement en vue d'obtenir des communications en lien avec l'étranger (y compris tout élément comportant de la parole, de la musique, des sons, des images visuelles ou les données d'une description), des données relatives aux équipements (des données qui permettent ou facilitent le fonctionnement d'un service postal, d'un système de télécommunications ou d'un service de télécommunications) ou toute autre information[367].

---

363 Les îles Britanniques se composent du Royaume-Uni, des îles Anglo-Normandes et de l'Île de Man et sont définies à l'annexe 1 de la loi d'interprétation de 1978, disponible à l'adresse suivante: https://www.legislation.gov.uk/ukpga/1978/30/schedule/1.

364 Conformément à l'article 136 de l'IPA 2016, les «communications en lien avec l'étranger» signifient: i) les communications envoyées par des personnes se trouvant en dehors des îles Britanniques, ou ii) les communications reçues par des personnes se trouvant en dehors des îles Britanniques. Ce régime, comme l'ont confirmé les autorités du Royaume-Uni, couvre également les communications entre deux personnes qui se trouvent toutes deux en dehors des îles Britanniques. La grande chambre de la Cour européenne des droits de l'homme dans l'affaire Big Brother Watch et autres/Royaume-Uni (voir note de bas de page 279 ci-dessus) a conclu, au point 376, en ce qui concerne une limitation similaire (faisant référence aux «communications externes») des communications pouvant être captées par une interception de masse au titre de la RIPA 2000, qu'elle était suffisamment délimitée et prévisible.

365 Article 136, paragraphe 4, de l'IPA 2016. Selon les explications fournies par le gouvernement britannique, l'interception de masse peut par exemple être utilisée pour identifier des menaces auparavant inconnues pour la sécurité nationale du Royaume-Uni, en filtrant et en analysant les éléments interceptés afin de repérer les communications susceptibles de présenter un intérêt pour le renseignement (section H du cadre explicatif du Royaume-Uni: Sécurité nationale, pages 27 et 28, voir la note de bas de page 29). Comme l'ont expliqué les autorités britanniques, ces instruments peuvent être utilisés pour établir des liens entre des sujets d'intérêt connus et pour chercher des traces d'activités menées par des personnes qui ne sont peut-être pas encore connues des services de renseignement mais qui peuvent apparaître dans le cadre d'une enquête, ainsi que pour identifier des types d'activité susceptibles d'indiquer l'existence d'une menace pour le Royaume-Uni.

366 Conformément à l'article 13, paragraphe 1, de l'IPA 2016, le recours à l'interférence avec des équipements par les services de renseignement doit être autorisé au moyen d'un mandat en vertu de l'IPA 2016, à condition qu'il existe une «connexion avec les îles Britanniques», voir le considérant (211).

367 Article 176 de l'IPA 2016. Un mandat d'interférence de masse avec des équipements ne peut pas autoriser une conduite qui constituerait (en l'absence d'une autorité légitime pour ce faire) une interception illégale (sauf en lien avec une communication conservée). Selon le cadre explicatif du Royaume-Uni, les informations obtenues pourraient être nécessaires à l'identification de sujets d'intérêt et relèveraient en général d'opérations de grande ampleur appropriées (cadre explicatif du Royaume-Uni, section H: Sécurité nationale, page 28, voir la note de bas de page 29).

(220) Le secrétaire d'État ne peut délivrer un mandat de masse que sur demande d'un directeur d'un service de renseignement[368]. Un mandat autorisant une interception de masse ou une interférence de masse avec des équipements ne doit être délivré que si cela est nécessaire dans l'intérêt de la sécurité nationale et aux fins supplémentaires de prévenir ou de détecter des infractions graves, ou dans l'intérêt de la prospérité économique du Royaume-Uni lorsque cet intérêt relève aussi de la sécurité nationale[369]. De plus, en vertu de l'article 142, paragraphe 7, de l'IPA 2016, un mandat d'interception de masse doit être plus précis qu'une simple référence aux «intérêts de la sécurité nationale», à la «prospérité économique du Royaume-Uni» et à la «prévention et la lutte contre des infractions graves», mais un lien doit être établi entre la mesure demandée et une ou plusieurs des finalités opérationnelles devant être incluses dans le mandat.

(221) Le choix de la finalité opérationnelle est le résultat d'un processus en plusieurs étapes. L'article 142, paragraphe 4, prévoit que les finalités opérationnelles mentionnées dans le mandat doivent être précisées dans une liste tenue à jour par les directeurs des services de renseignement et être considérées par ces derniers comme des finalités opérationnelles pour lesquelles les contenus interceptés ou les données secondaires obtenues dans le cadre de mandats d'interception de masse peuvent être sélectionnés en vue de leur examen. La liste des finalités opérationnelles doit être approuvée par le secrétaire d'État. Le secrétaire d'État ne peut donner cette approbation qu'après s'être assuré que la finalité opérationnelle est décrite de manière plus détaillée que les motifs généraux d'autorisation des mandats (sécurité nationale ou sécurité nationale et prospérité économique ou prévention des infractions graves)[370]. À l'issue de chaque période correspondante de trois mois, le secrétaire d'État doit donner une copie de la liste des finalités opérationnelles à la commission parlementaire sur le renseignement et la sécurité. Enfin, le Premier ministre doit examiner la liste des finalités opérationnelles au moins une fois par an[371]. Comme l'a fait observer la Haute Cour, «[c]es garanties ne doivent pas être dépréciées et considérées comme des garanties insignifiantes, étant donné qu'elles constituent à elles toutes un ensemble complexe de modes de responsabilisation, qui impliquent le Parlement et les membres du gouvernement au plus haut niveau»[372].

(222) Ces finalités opérationnelles limitent également la portée de la sélection des éléments interceptés en vue de la phase d'examen. La sélection des éléments collectés en vertu du mandat de masse en vue de leur examen doit être justifiée au regard des finalités opérationnelles. Comme l'ont expliqué les autorités britanniques, cela signifie que le secrétaire d'État doit évaluer les modalités pratiques d'examen dès l'étape du mandat et qu'il doit disposer de suffisamment d'informations détaillées pour respecter les obligations légales prévues aux articles 152 et 193 de l'IPA 2016[373]. Les informations

368 Article 138, paragraphe 1, et article 178, paragraphe 1, de l'IPA 2016.

369 Article 138, paragraphe 2, et article 178, paragraphe 2, de l'IPA 2016.

370 Selon les explications fournies par les autorités britanniques, une finalité opérationnelle peut, par exemple, limiter la portée de la mesure à l'existence d'une menace dans une zone géographique donnée.

371 Article 142, paragraphes 4 à 10, de l'IPA 2016.

372 Haute Cour de Justice, arrêt Liberty, [2019] EWHC 2057 (Admin), point 167.

373 Les articles 152 et 193 de l'IPA 2016 exigent que: a) la sélection en vue de l'examen ne soit réalisée que pour les finalités opérationnelles précisées dans le mandat, b) la sélection en vue de l'examen soit nécessaire et proportionnée en toutes circonstances, et c) la sélection en vue de l'examen n'enfreigne pas l'interdiction de sélectionner des éléments et d'identifier des communications envoyées par ou destinées à des personnes dont on sait qu'elles se trouvaient dans les îles Britanniques à ce moment.

détaillées fournies au secrétaire d'État en lien avec ces dispositions doivent par exemple inclure des informations (le cas échéant) sur la manière dont les dispositions de filtrage peuvent varier pendant la durée de validité du mandat[374]. Pour de plus amples informations sur le déroulement des phases de filtrage et d'examen et les garanties qui s'y appliquent, voir le considérant (229) below ci-dessous.

(223) Un pouvoir de masse ne peut être autorisé que s'il est proportionné à l'objectif visé[375]. Comme le précise le code de bonnes pratiques relatif à l'interception, toute appréciation de la proportionnalité nécessite de «mettre en balance la gravité de l'intrusion dans la vie privée (et les autres considérations mentionnées à l'article 2, paragraphe 2) avec la nécessité de l'activité du point de vue de l'enquête, des besoins opérationnels ou des capacités. La conduite autorisée devrait offrir une perspective réaliste d'apporter les avantages escomptés et ne devrait être ni disproportionnée, ni arbitraire»[376]. Comme indiqué précédemment, cela signifie en pratique que le critère de proportionnalité est fondé sur un critère d'équilibre entre l'objectif visé («la finalité opérationnelle») et les options techniques disponibles (par ex. interception ciblée ou de masse, interférence ciblée ou de masse avec des équipements, acquisition ciblée ou de masse de données de communication), la préférence devant être donnée aux moyens les moins intrusifs (voir les considérants (181) et (182) above ci-dessus). Lorsque plusieurs mesures sont appropriées au regard de l'objectif, le moyen le moins intrusif doit être privilégié.

(224) Le fait que le secrétaire d'État doive recevoir les informations utiles nécessaires à la bonne réalisation de son évaluation constitue une garantie supplémentaire concernant l'appréciation de la proportionnalité de la mesure demandée. Le code de bonnes pratiques relatif à l'interception et le code de bonnes pratiques relatif à l'interférence avec des équipements exigent notamment que la demande présentée par l'autorité compétente contienne une description du contexte de la demande, une description des communications devant être interceptées et des opérateurs de télécommunications dont l'aide est requise, une description de la conduite devant être autorisée, une description des finalités opérationnelles et une explication de la raison pour laquelle la conduite est nécessaire et proportionnée[377].

(225) Enfin et surtout, la décision du secrétaire d'État de délivrer le mandat doit être approuvée par un commissaire judiciaire indépendant, qui évalue l'appréciation de la nécessité et de la proportionnalité de la mesure proposée au regard des mêmes principes que le ferait un tribunal en cas de demande de contrôle juridictionnel[378]. Plus

374 Voir le point 6.6 du code de bonnes pratiques relatif à l'interception des communications, voir la note de bas de page 278.

375 Article 138, paragraphe 1, points b) et c), et article 178, points b) et c), de l'IPA 2016.

376 Point 4.10 du code de bonnes pratiques relatif à l'interception des communications, voir la note de bas de page 278.

377 Point 6.20 du code de bonnes pratiques relatif à l'interception des communications, voir la note de bas de page 278, et point 6.13 du code de bonnes pratiques relatif à l'interférence avec des équipements, voir la note de bas de page 348.

378 Article 138, paragraphe 1, point g), et article 178, paragraphe 1), point f), de l'IPA 2016. La Cour européenne des droits de l'homme a notamment considéré que l'autorisation préalable d'un organe indépendant constituait une garantie importante contre les abus dans le cadre de l'interception de masse. Cour européenne des droits de l'homme (grande chambre), Big Brother Watch et autres/Royaume-Uni (voir note 269 ci-dessus), points 351 et 352. Il importe de garder à l'esprit que cet arrêt concernait le cadre juridique antérieur (RIPA 2000) qui ne contenait pas certaines des garanties (y compris l'autorisation préalable d'un commissaire judiciaire indépendant) introduites par l'IPA 2016.

précisément, le commissaire judiciaire examinera les conclusions du secrétaire d'État déterminant si le mandat est nécessaire et si la conduite est proportionnée au regard des principes énoncés à l'article 2, paragraphe 2, de l'IPA 2016 (obligations générales relatives à la protection de la vie privée). Le commissaire judiciaire examinera également les conclusions du secrétaire d'État déterminant si chacune des finalités opérationnelles mentionnées dans le mandat constitue une finalité pour laquelle la sélection est ou pourrait être nécessaire. Si le commissaire judiciaire refuse d'approuver la décision de délivrer un mandat, le secrétaire d'État peut: i) accepter la décision et donc ne pas délivrer le mandat ou ii) renvoyer la question devant le commissaire aux pouvoirs d'enquête, qui tranchera (sauf si c'est le commissaire aux pouvoirs d'enquête qui a pris la décision initiale)[379].

ii) Garanties supplémentaires

(226) L'IPA 2016 a introduit des limitations supplémentaires en ce qui concerne la durée, le renouvellement et la modification d'un mandat de masse. Le mandat doit avoir une durée maximale de six mois et toute décision de le renouveler ou de le modifier (à l'exception de modifications mineures) doit également être approuvée par un commissaire judiciaire[380]. Le code de bonnes pratiques relatif à l'interception et le code de bonnes pratiques relatif à l'interférence avec des équipements précisent qu'une modification apportée aux finalités opérationnelles du mandat est considérée comme une modification majeure de ce dernier[381].

(227) À l'instar des dispositions relatives à l'interception ciblée, la partie 6 de l'IPA 2016 prévoit que le secrétaire d'État doit veiller à ce que des dispositions soient en vigueur pour apporter les garanties nécessaires concernant la conservation et la divulgation des éléments obtenus en vertu du mandat[382], ainsi que la divulgation à l'étranger[383]. L'article 150, paragraphe 5, et l'article 191, paragraphe 5, de l'IPA 2016 exigent notamment que toute copie faite des éléments collectés en vertu du mandat soit stockée de manière sécurisée et détruite dès qu'il n'existe plus de motifs pertinents de la conserver, tandis que l'article 150, paragraphe 2, et l'article 191, paragraphe 2, exigent que le nombre de personnes à qui sont divulgués ces éléments et la mesure dans laquelle ces éléments sont divulgués, mis à disposition ou copiés soient limités au minimum nécessaire aux fins prévues par la loi[384].

---

379 Article 159, paragraphes 3 et 4, de l'IPA 2016.

380 Articles 143 à 146 et articles 184 à 188 de l'IPA 2016. En cas de modification urgente, le secrétaire d'État peut procéder à la modification sans approbation, mais il doit le notifier au commissaire et celui-ci doit ensuite décider d'approuver ou de refuser la modification (article 147 de l'IPA 2016). Les mandats doivent être annulés lorsqu'ils ne sont plus nécessaires ou proportionnés ou lorsque l'examen des contenus, métadonnées ou autres données interceptés en vertu du mandat n'est plus nécessaire à aucune des finalités opérationnelles mentionnées dans le mandat (articles 148 et 189 de l'IPA 2016).

381 Points 6.44 à 6.47 du code de bonnes pratiques relatif à l'interception des communications, voir la note de bas de page 278, et point 6.48 du code de bonnes pratiques relatif à l'interférence avec des équipements, voir la note de bas de page 348.

382 Article 156 de l'IPA 2016.

383 Articles 150 et 191 de l'IPA 2016.

384 La grande chambre de la Cour européenne des droits de l'homme dans l'affaire Big Brother Watch et autres/Royaume-Uni (voir note de bas de page 268ci-dessus) a confirmé le système de garanties supplémentaires en matière de conservation, d'accès et de divulgation qui avait été mis en place au titre de la RIPA 2000 (voir points 392 à 394 et 402 à 405). Le même système de garanties est prévu par l'IPA 2016.

(228) Enfin, lorsque les éléments qui ont été interceptés dans le cadre d'une interception de masse ou d'une interférence de masse avec des équipements doivent être remis à un pays tiers («divulgation à l'étranger»), l'IPA 2016 impose au secrétaire d'État de veiller à ce que des dispositions appropriées soient en vigueur afin d'assurer que des garanties similaires en matière de sécurité, de conservation et de divulgation existent dans le pays en question[385]. De plus, l'article 109 de la DPA 2018 définit des exigences spécifiques applicables aux transferts internationaux de données à caractère personnel par les services de renseignement vers des pays tiers ou à des organisations internationales, et ne permet pas que les données à caractère personnel soient transférées vers un pays ou un territoire en dehors du Royaume-Uni ou à une organisation internationale, sauf si ce transfert est nécessaire et proportionné aux fins de l'exercice des fonctions réglementaires du responsable du traitement ou aux autres fins prévues par l'article 2, paragraphe 2, point a), de la loi de 1989 sur les services de sécurité ou par l'article 2, paragraphe 2, point a), et par l'article 4, paragraphe 2, point a), de la loi de 1994 sur les services de renseignement[386]. Il est important de noter que ces exigences s'appliquent également dans les cas où l'exemption concernant la sécurité nationale prévue à l'article 110 de la DPA de 2018 est invoquée, étant donné que l'article 110 de la DPA de 2018 ne mentionne pas l'article 109 de la DPA de 2018 parmi les dispositions pouvant être écartées si une dérogation à certaines dispositions est nécessaire pour préserver la sécurité nationale.

(229) Une fois que le mandat a été approuvé et que les données ont été collectées en masse, les données feront l'objet d'une sélection avant d'être examinées. La phase de sélection et d'examen est soumise à un critère de proportionnalité supplémentaire appliqué par l'analyste qui définit, sur la base des finalités opérationnelles incluses dans le mandat (et des éventuelles dispositions de filtrage existantes), les critères de sélection. Comme le prévoient les articles 152 et 193 de l'IPA, lorsqu'il délivre le mandat, le secrétaire d'État doit veiller à ce que des dispositions soient en vigueur pour garantir que la sélection des éléments n'est effectuée que pour les finalités opérationnelles prévues et qu'elle est nécessaire et proportionnée en toutes circonstances. À cet égard, les autorités britanniques ont précisé que les éléments interceptés en masse sont tout d'abord sélectionnés au moyen d'un filtrage automatique, en vue d'écarter les données qui sont peu susceptibles d'avoir un intérêt pour la sécurité nationale. Les filtres varient de temps à autre (à mesure que les modes, les types et les protocoles de trafic sur internet évoluent) et dépendent de la technologie et du contexte opérationnel. Après cette phase, les données ne peuvent être sélectionnées en vue de leur examen que si elles sont pertinentes pour les finalités opérationnelles précisées dans le mandat[387]. Les garanties prévues par l'IPA 2016 pour

385 Articles 151 et 192 de l'IPA 2016.

386 Pour de plus amples informations à ce sujet, voir la note de bas de page 312.

387 Le code de bonnes pratiques relatif à l'interception des communications précise, à cet égard, que «[c]es systèmes de traitement traitent les données à partir des liens ou des signaux de communication que l'autorité qui intercepte les données a choisi d'intercepter. Un certain degré de filtrage est ensuite appliqué au trafic sur ces liens et signaux, pour sélectionner les types de communication qui sont susceptibles de présenter un intérêt pour le renseignement, tout en rejetant ceux qui sont les moins susceptibles d'être intéressants à cet égard. À la suite de ce filtrage, qui varie d'un système de traitement à l'autre, une part considérable des communications sur ces liens et signaux sera automatiquement écartée. D'autres recherches complexes peuvent ensuite être effectuées afin d'extraire les communications les plus susceptibles de présenter un intérêt pour le renseignement, qui sont liées aux pouvoirs réglementaires de l'agence concernée. Ces communications peuvent ensuite être sélectionnées en vue de leur examen pour une ou plusieurs des finalités opérationnelles précisées dans le mandat

l'examen des éléments collectés s'appliquent à tout type de données (contenus interceptés et données secondaires)[388]. Les articles 152 et 193 de l'IPA 2016 interdisent également de manière générale de sélectionner en vue de leur examen des éléments portant sur des communications envoyées par ou destinées à des personnes se trouvant dans les îles Britanniques. Si les autorités souhaitent examiner ces éléments, elles doivent demander un mandat d'examen ciblé au titre de la partie 2 et de la partie 4 de l'IPA 2016, qui est délivré par le secrétaire d'État et approuvé par un commissaire judiciaire[389]. Si une personne sélectionne délibérément des contenus interceptés en vue de leur examen sans respecter les exigences prévues par la loi[390], elle commet une infraction pénale[391].

(230) L'analyse de la sélection des éléments réalisée par l'analyste est soumise à une surveillance ex post de l'IPC, qui évalue la conformité avec les garanties spécifiques prévues par l'IPA 2016 en ce qui concerne la phase d'examen[392] (voir également le considérant (229)). L'IPC doit examiner (y compris au moyen d'audits, d'inspections et d'enquêtes) l'exercice par les autorités publiques des pouvoirs d'enquête mentionnés dans l'IPA 2016[393]. À cet égard, le code de bonnes pratiques relatif à l'interception et le code de bonnes pratiques relatif à l'interférence avec des équipements précisent que l'agence doit tenir des registres en vue de l'examen ultérieur et des audits et que ces registres doivent indiquer les raisons pour lesquelles l'accès aux éléments par des personnes autorisées est nécessaire et proportionné, ainsi que les finalités opérationnelles applicables[394]. Par exemple, dans son rapport annuel de 2018, le Bureau du commissaire aux pouvoirs d'enquête[395] a conclu que les justifications enregistrées par les analystes en vue de l'examen de certains éléments collectés en masse étaient conformes au critère de proportionnalité requis en détaillant suffisamment les raisons de leurs «demandes» en lien avec l'objectif visé[396]. Dans son rapport de 2019, l'IPCO, en ce qui concerne les pouvoirs de masse, a clairement fait part de son intention de poursuivre les inspections relatives aux interceptions de

---

lorsque les conditions de nécessité et de proportionnalité sont remplies. Seules les données qui n'ont pas été écartées peuvent être sélectionnées en vue de leur examen par des personnes autorisées» (point 6.6 du code de bonnes pratiques relatif à l'interception des communications, voir la note de bas de page 278).

388 Voir l'article 152, paragraphe 1, points a) et b), de l'IPA 2016 selon lequel l'examen des deux types de données (contenus interceptés et données secondaires) n'est effectué que pour les finalités opérationnelles prévues et doit être nécessaire et proportionné en toutes circonstances.

389 Ce type de mandat n'est pas requis lorsque les données relatives aux personnes se trouvant dans les îles Britanniques sont des «données secondaires» (voir l'article 152, paragraphe 1), point c), de l'IPA 2016.

390 Articles 152 et 193 de l'IPA 2016.

391 Articles 155 et 196 de l'IPA 2016.

392 Articles 152 et 193 de l'IPA 2016.

393 Article 229 de l'IPA 2016.

394 Point 6.74 du code de bonnes pratiques relatif à l'interception des communications, voir la note de bas de page 278, et point 6.78 du code de bonnes pratiques relatif à l'interférence avec des équipements, voir la note de bas de page 348.

395 L'IPCO est constitué en vertu de l'article 238 de l'IPA 2016 afin de fournir à l'IPC le personnel, les locaux, les équipements et les autres installations et services nécessaires à l'exécution de ses missions (voir le considérant (251)).

396 Le rapport annuel de 2018 de l'IPCO précisait que les justifications enregistrées par les analystes du GCHQ «respectaient les critères requis et les analystes rendaient compte de la proportionnalité de leurs demandes de collecte en masse de manière suffisamment détaillée». Point 6.22 du rapport annuel de 2018 du commissaire aux pouvoirs d'enquête, voir la note de bas de page 464.

masse, y compris un examen détaillé des sélecteurs et des critères de recherche[397]. Il continuera également à examiner attentivement, au cas par cas, le choix des mesures de surveillance (ciblées ou de masse) tant lors de l'examen des demandes de mandat suivant la procédure «de double verrouillage» que lors des inspections[398]. Cette surveillance supplémentaire sera dûment prise en compte dans le cadre du suivi de la présente décision par la Commission visé aux considérants (281)à(284).

3.3.1.1.4.2 Acquisition de masse de données de communication

(231) Le chapitre 2 de la partie 6 de l'IPA 2016 régit les mandats d'acquisition de masse qui autorisent leur destinataire à demander à un opérateur de télécommunications de divulguer ou d'obtenir des données de communication en possession de ce dernier. Ces mandats autorisent également l'autorité requérante à sélectionner les données en vue de la phase ultérieure d'examen. À l'instar de la conservation et de l'acquisition ciblées de données de communication (voir le considérant (199) ci-dessus), généralement, l'acquisition de masse de données de communication ne concerne pas les données à caractère personnel de personnes concernées de l'Union européenne transférées vers le Royaume-Uni au titre de la présente décision. L'obligation de divulguer les données de communication au titre de la partie 6, chapitre 2, de l'IPA 2016 couvre les données collectées par les opérateurs de télécommunications au Royaume-Uni directement auprès des utilisateurs d'un service de télécommunications[399]. Généralement, ce type de traitement «en contact avec la clientèle» n'implique pas un transfert au titre de la présente décision, c.-à-d. un transfert d'un responsable du traitement/sous-traitant de l'Union à un responsable du traitement/sous-traitant au Royaume-Uni.

(232) Cependant, par souci d'exhaustivité, les conditions et garanties régissant l'acquisition de données de communication de masse sont décrites ci-dessous.

---

397 Point 7.6 du rapport annuel de 2019 du commissaire aux pouvoirs d'enquête, voir la note de bas de page 463.

398 Point 10.22 du rapport annuel de 2019 du commissaire aux pouvoirs d'enquête, voir la note de bas de page 463.

399 Cela découle de la définition des données de communication contenue à l'article 261, paragraphe 5, de l'IPA 2016, selon laquelle les données de communication sont détenues ou obtenues par un opérateur de télécommunications et soit portent sur l'utilisateur d'un service de télécommunication et sur la fourniture de ce service, soit sont comprises dans une communication, en font partie, y sont jointes ou logiquement associées (voir également le code de bonnes pratiques relatif à l'acquisition de masse de données de communication, disponible à l'adresse suivante: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf, points 2.15 à 2.22). De plus, selon la définition d'un «opérateur de télécommunications» proposée à l'article 261, paragraphe 10, de l'IPA 2016, il doit s'agir d'une personne qui propose ou fournit un service de télécommunications à des personnes au Royaume-Uni ou qui contrôle ou fournit un système de télécommunications se trouvant au Royaume-Uni ou contrôlé depuis ce pays (entièrement ou en partie). Ces définitions indiquent clairement que les obligations au titre de l'IPA 2016 ne peuvent pas être imposées aux opérateurs de télécommunications dont les équipements ne se trouvent pas au Royaume-Uni ou ne sont pas contrôlés depuis ce pays ou qui ne proposent ou ne fournissent pas de services à des personnes se trouvant au Royaume-Uni (voir également le code de bonnes pratiques relatif à l'acquisition de masse de données de communication, point 2.2). Si des abonnés de l'Union (qu'ils se trouvent dans l'Union ou au Royaume-Uni) ont recours à des services au Royaume-Uni, toute donnée de communication en lien avec la fourniture de ce service sera collectée directement par le fournisseur de services au Royaume-Uni plutôt que de faire l'objet d'un transfert depuis l'Union.

(233) L'IPA 2016 remplace la législation relative à l'acquisition de données de communication de masse qui était l'objet de l'arrêt rendu par la CJUE dans l'affaire Privacy International. La législation en cause dans cette affaire a été abrogée et le nouveau régime prévoit des conditions et des garanties spécifiques en vertu desquelles une telle mesure peut être autorisée.

(234) En particulier, contrairement au régime précédent selon lequel le secrétaire d'État disposait d'un pouvoir discrétionnaire absolu pour autoriser la mesure[400], en vertu de l'IPA 2016, le secrétaire d'État ne peut délivrer un mandat que si la mesure est nécessaire et proportionnée. Cela signifie en pratique qu'il devrait y avoir un lien entre l'accès aux données et l'objectif poursuivi[401]. Plus précisément, le secrétaire d'État devra évaluer l'existence d'un lien entre la mesure demandée et l'une ou plusieurs des «finalités opérationnelles» mentionnées dans le mandat (voir le considérant 219 ci-dessus). S'agissant de l'appréciation de la proportionnalité, le code de bonnes pratiques applicable précise que «le secrétaire d'État doit déterminer si l'objectif visé par le mandat pourrait être raisonnablement atteint par d'autres moyens moins intrusifs [article 2, paragraphe 2, point a), de la loi]. Par exemple, l'obtention des informations nécessaires par un pouvoir moins intrusif tel que l'acquisition ciblée de données de communication»[402].

(235) Pour réaliser une telle appréciation, le secrétaire d'État s'appuie sur les informations que les directeurs des services de renseignement[403] sont tenus de fournir dans leur demande, comme les raisons pour lesquelles la mesure est jugée nécessaire pour l'un des motifs prévus par la loi ou les raisons pour lesquelles l'objectif visé ne pourrait pas être raisonnablement atteint par d'autres moyens moins intrusifs[404]. De plus, les finalités opérationnelles limitent la mesure dans laquelle les données obtenues en vertu du mandat peuvent être sélectionnées en vue de leur examen[405]. Comme le précise le code de bonnes pratiques applicable, les finalités opérationnelles doivent décrire une exigence claire et être suffisamment détaillées pour convaincre le secrétaire d'État que les données acquises ne peuvent être sélectionnées en vue de leur examen que pour des raisons spécifiques[406]. En réalité, le secrétaire d'État devra s'assurer, avant d'autoriser le mandat, que des dispositions spécifiques sont en vigueur afin de garantir que seuls les éléments dont l'examen est considéré comme nécessaire pour une finalité opérationnelle et une finalité prévue par la loi sont sélectionnés en vue de leur examen

---

400 L'article 94, paragraphe 1, de la loi de 1984 sur les télécommunications prévoyait que le secrétaire d'État pouvait donner «des instructions de nature générale lui semblant nécessaires ou utiles dans l'intérêt de la sécurité nationale […]» (voir la note de bas de page 451).

401 Voir l'arrêt Privacy International, point 78.

402 Voir le point 4.11 du code de bonnes pratiques relatif à l'acquisition de masse des données de communication (voir la note de bas de page 399414).

403 Un mandat d'acquisition de masse ne peut être demandé que par les directeurs des services de renseignement, qui sont: i) le directeur général du MI5; ii) le chef du SIS; ou iii) le directeur du GCHQ (voir les articles 158 et 263 de l'IPA 2016).

404 Point 4.5 du code de bonnes pratiques relatif à l'acquisition de masse des données de communication (voir la note de bas de page 399).

405 Selon l'article 161 de l'IPA 2016, les finalités opérationnelles mentionnées dans le mandat doivent être précisées dans une liste tenue à jour par les directeurs des services de renseignement (la «liste des finalités opérationnelles») et être considérées par ces derniers comme des finalités opérationnelles pour lesquelles les données de communication obtenues dans le cadre de mandats d'acquisition de masse peuvent être sélectionnées en vue de leur examen.

406 Point 6.6 du code de bonnes pratiques relatif à l'acquisition de masse des données de communication (voir la note de bas de page 399).

et que les principes de proportionnalité et de nécessité sont respectés en toutes circonstances. Cette exigence spécifique, qui figure aux articles 158 et 172[407] de l'IPA 2016, concernant l'appréciation préalable de la nécessité et de la proportionnalité des critères utilisés aux fins de la sélection, constitue une autre nouveauté importante du régime instauré par cette loi par rapport au régime précédent.

(236) L'IPA 2016 oblige également le secrétaire d'État à s'assurer que, avant de délivrer le mandat d'acquisition de masse de données de communication, des limitations spécifiques sont en place concernant la sécurité, la conservation et la divulgation des données à caractère personnel collectées[408]. En cas de divulgation à l'étranger, les garanties décrites au considérant (227) pour l'interception de masse et l'interférence de masse avec des équipements s'appliquent également dans ce contexte[409]. La législation prévoit des limitations supplémentaires concernant la durée[410], le renouvellement[411] et la modification des mandats de masse[412].

(237) Il est important de noter que, tout comme pour les autres pouvoirs de masse, avant de délivrer le mandat, le secrétaire d'État doit obtenir l'approbation d'un commissaire judiciaire[413]. Il s'agit là de l'une des caractéristiques essentielles du régime mis en place par l'IPA 2016.

(238) L'IPC assure une surveillance ex post de la procédure d'examen concernant les éléments (données de communication) acquis en masse (voir le considérant (254) below ci-dessous). À cet égard, en vertu de l'IPA 2016, l'analyste du service de renseignement réalisant l'examen doit consigner, avant la sélection des données en vue de leur examen, la raison pour laquelle l'examen envisagé est nécessaire et proportionné à la finalité opérationnelle spécifiée[414]. Dans le rapport annuel de 2019 de l'IPCO, il a été conclu au sujet des pratiques du GCHQ et du MI5 que «le rôle essentiel joué par les données de communication en masse dans l'ensemble des activités menées au GCHQ était bien articulé dans les dossiers que nous avons inspectés. Nous avons examiné la nature des données demandées et les exigences énoncées en matière de renseignement et selon nos conclusions, la documentation démontrait que leur approche était nécessaire et proportionnée»[415]. «Les justifications enregistrées par le MI5 étaient de qualité et respectaient les principes de nécessité et de proportionnalité»[416].

3.3.1.1.4.3 Conservation et examen d'ensembles de données à caractère personnel en masse

---

407 L'article 172 de l'IPA 2016 exige que des garanties spécifiques soient mises en place pour la phase de filtrage et de sélection en vue de l'examen des communications acquises en masse. De plus, un examen réalisé de manière délibérée en violation de ces garanties constitue également une infraction pénale (voir l'article 173 de l'IPA 2016).

408 Article 171 de l'IPA 2016.

409 Article 171, paragraphe 9, de l'IPA 2016.

410 Article 162 de l'IPA 2016.

411 Article 163 de l'IPA 2016.

412 Articles 164 à 166 de l'IPA 2016.

413 Article 159 de l'IPA 2016.

414 Point 8.6 du rapport annuel de 2019 de l'IPCO, voir la note de bas de page 463.

415 Point 10.4 du rapport annuel de 2019 de l'IPCO, voir la note de bas de page 463.

416 Point 8.37 du rapport annuel de 2019 de l'IPCO, voir la note de bas de page 463.

(239) Les mandats relatifs aux ensembles de données à caractère personnel en masse (EDM)[417] 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. Selon les explications fournies par les autorités britanniques, l'analyse de ces ensembles de données peut être «le seul moyen pour la communauté du renseignement britannique de faire avancer les enquêtes et d'identifier des terroristes à partir de renseignements majeurs très limités ou lorsque leurs communications ont été délibérément dissimulées»[418]. Il existe deux types de mandats: «les mandats EDM par catégorie»[419], qui concernent une certaine catégorie d'ensembles de données, à savoir des ensembles de données dont le contenu et l'utilisation envisagée sont similaires et qui soulèvent des questions similaires concernant, par exemple, le degré d'intrusion et de sensibilité, ainsi que le caractère proportionné de l'utilisation des données, ce qui permet au secrétaire d'État d'examiner la nécessité et la proportionnalité de l'acquisition de l'intégralité des données relevant de la catégorie concernée en une seule fois. Par exemple, un mandat EDM par catégorie peut couvrir des ensembles de données de déplacement qui portent sur des itinéraires similaires[420]. Les «mandats EDM spécifiques»[421] concernent eux un ensemble de données spécifique, tel qu'un ensemble de données comportant un type d'informations nouveau ou inhabituel qui ne relève pas d'un mandat EDM par catégorie existant, ou un ensemble de données qui concerne certains types spécifiques de données à caractère personnel[422] et qui nécessite donc des garanties supplémentaires[423]. Les dispositions de l'IPA 2016 relatives aux EDM ne permettent d'examiner et de conserver ces ensembles de données que si ces actions sont nécessaires et proportionnées[424] et si elles respectent les obligations générales relatives à la protection de la vie privée[425].

(240) Le pouvoir de délivrer un mandat EDM est soumis à la procédure «de double verrouillage»: l'appréciation de la nécessité et de la proportionnalité de la mesure est

---

417 Article 200 de l'IPA 2016.

418 Cadre explicatif relatif aux discussions sur l'adéquation du Royaume-Uni, section H: Sécurité nationale, page 34, voir la note de bas de page 29.

419 Article 204 de l'IPA 2016.

420 Point 4.7 du code de bonnes pratiques relatif à la conservation et à l'utilisation par les services de renseignement des ensembles de données à caractère personnel en masse, disponible à l'adresse suivante: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715478/Bulk_Personal_Datasets_Code_of_Practice.pdf

421 Article 205 de l'IPA 2016.

422 Par exemple, les données à caractère personnel sensibles, voir l'article 202 de l'IPA 2016 et les points 4.21 et 4.12 du code de bonnes pratiques relatif à la conservation et à l'utilisation par les services de renseignement des ensembles de données à caractère personnel en masse, voir la note de bas de page 469.

423 Une demande de mandat EDM spécifique doit faire l'objet d'un examen individuel par le secrétaire d'État, c.-à-d. à l'égard d'un ensemble de données spécifique. En vertu de l'article 205 de l'IPA, le service de renseignement est tenu d'inclure dans sa demande de mandat EDM spécifique une explication détaillée de la nature et de la portée des éléments en question, ainsi qu'une liste des «finalités opérationnelles» pour lesquelles le service de renseignement en question souhaite examiner l'EDM (lorsque le service de renseignement demande un mandat de conservation et d'examen, et pas uniquement un mandat de conservation). En revanche, lorsqu'il délivre un mandat EDM par catégorie, le secrétaire d'État examine en une seule fois l'intégralité de la catégorie d'ensembles de données.

424 Articles 204 et 205 de l'IPA 2016.

425 Article 2 de l'IPA 2016.

tout d'abord réalisée par le secrétaire d'État, puis par le commissaire judiciaire[426]. Le secrétaire d'État doit tenir compte de la nature et du champ d'application du type de mandat demandé, de la catégorie de données concernée et du nombre d'ensembles de données à caractère personnel en masse susceptibles de relever du champ d'application du type spécifique de mandat[427]. De même, comme le prévoit le code de bonnes pratiques relatif à la conservation et à l'utilisation par les services de renseignement des ensembles de données à caractère personnel en masse, des registres détaillés doivent être tenus et sont soumis au contrôle de l'IPC[428]. Le fait de conserver et d'examiner des EDM en dehors des limitations prévues par l'IPA 2016 constitue une infraction pénale[429].

3.3.2 Utilisation ultérieure des informations recueillies

(241) Les données à caractère personnel traitées en vertu de la partie 4 de la DPA 2018 ne doivent pas être traitées d'une manière incompatible avec la finalité pour laquelle elles ont été collectées[430]. La DPA 2018 prévoit que le responsable du traitement peut traiter les données pour une finalité différente de celle pour laquelle elles ont été collectées lorsqu'elle est compatible avec la finalité initiale et à condition que le responsable du traitement soit légalement autorisé à traiter les données et que le traitement soit nécessaire et proportionné[431]. De plus, la loi de 1989 sur les services de sécurité et la loi de 1994 sur les services de renseignement précisent que les directeurs des agences de renseignement doivent s'assurer qu'aucune information n'est obtenue ou divulguée sauf dans la mesure où cela est nécessaire à la bonne exécution des missions de l'agence ou aux autres finalités limitées et spécifiques énumérées dans les dispositions en vigueur[432].

(242) De plus, l'article 109 de la DPA 2018 définit des exigences spécifiques applicables aux transferts internationaux de données à caractère personnel par les services de renseignement vers des pays tiers ou à des organisations internationales. Selon cette disposition, les données à caractère personnel ne peuvent pas être transférées vers un pays ou un territoire en dehors du Royaume-Uni ou à une organisation internationale, sauf si ce transfert est nécessaire et proportionné aux fins de l'exercice des fonctions

426 Articles 204 et 205 de l'IPA 2016.

427 Point 5.2 du code de bonnes pratiques relatif à la conservation et à l'utilisation par les services de renseignement des ensembles de données à caractère personnel en masse, voir la note de bas de page 420.

428 Points 8.1 à 8.15 du code de bonnes pratiques relatif à la conservation et à l'utilisation par les services de renseignement des ensembles de données à caractère personnel en masse, voir la note de bas de page 420.

429 Cadre explicatif relatif aux discussions sur l'adéquation du Royaume-Uni, section H: Sécurité nationale, page 34, voir la note de bas de page 29.

430 Article 87, paragraphe 1, de la DPA 2018.

431 Article 87, paragraphe 3, de la DPA 2018. Bien que les responsables du traitement puissent déroger à ce principe au titre de l'article 110 de la DPA 2018 dans la mesure où une telle dérogation est requise pour garantir la sécurité nationale, la dérogation doit être évaluée au cas par cas et ne peut être invoquée que dans la mesure où l'application d'une disposition particulière aurait des conséquences négatives sur la sécurité nationale (voir le considérant (132)). Les certificats de sécurité nationale pour les services de renseignement britanniques (disponibles à l'adresse suivante: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/) ne couvrent pas l'article 87, paragraphe 3, de la DPA 2018. De plus, étant donné que tout traitement pour une finalité différente doit être autorisé par la loi, les services de renseignement doivent disposer d'une base juridique claire concernant le traitement ultérieur.

432 Pour de plus amples informations à ce sujet, voir la note de bas de page 312.

réglementaires du responsable du traitement ou aux autres fins prévues par l'article 2, paragraphe 2, point a), de la loi de 1989 sur les services de sécurité ou par l'article 2, paragraphe 2, point a), et par l'article 4, paragraphe 2, point a), de la loi de 1994 sur les services de renseignement[433]. Il est important de noter que ces exigences s'appliquent également dans les cas où l'exemption concernant la sécurité nationale prévue à l'article 110 de la DPA de 2018 est invoquée, étant donné que l'article 110 de la DPA de 2018 ne mentionne pas l'article 109 de la DPA de 2018 parmi les dispositions pouvant être écartées si une dérogation à certaines dispositions est nécessaire pour préserver la sécurité nationale.

(243) Par ailleurs, comme l'a souligné l'ICO dans ses orientations sur le traitement des services de renseignement, outre les garanties prévues par la partie 4 de la DPA de 2018, une agence de renseignement, lorsqu'elle partage des données avec un service de renseignement d'un pays tiers, est également soumise à des garanties prévues par d'autres mesures législatives qui lui sont applicables afin de garantir que les données à caractère personnel sont obtenues, partagées et traitées de manière licite et responsable[434]. Par exemple, l'IPA 2016 définit des garanties supplémentaires en ce qui concerne les transferts vers un pays tiers des éléments collectés dans le cadre de l'interception ciblée[435], de l'interférence ciblée avec des équipements[436], de l'interception de masse[437], de l'acquisition de masse de données de communication[438] et de l'interférence de masse avec des équipements[439] (les «divulgations à l'étranger»). L'autorité délivrant le mandat doit notamment veiller à ce que des dispositions soient en vigueur pour garantir que le pays tiers destinataire des données limite au minimum nécessaire pour les finalités autorisées énoncées dans l'IPA 2016 le nombre de personnes qui consultent les éléments, la portée de la divulgation et le nombre de copies faites des éléments[440].

3.3.3 Surveillance

(244) Différents organes surveillent l'accès des pouvoirs publics à des fins de sécurité nationale. Le commissaire à l'information surveille le traitement des données à caractère personnel à la lumière de la DPA 2018 (pour de plus amples informations sur l'indépendance, le rôle de nomination et les pouvoirs du commissaire, voir les considérants (85) à (98)), tandis que l'IPC est responsable de la surveillance

433 Voir la note de bas de page 312.

434 Orientations de l'ICO sur le traitement des services de renseignement (voir la note de bas de page 161).

435 Article 54 de l'IPA 2016.

436 Article 130 de l'IPA 2016.

437 Article 151 de l'IPA 2016.

438 Article 171, paragraphe 9, de l'IPA 2016.

439 Article 192 de l'IPA 2016.

440 Les dispositions doivent comprendre des mesures visant à garantir que toute copie faite des éléments est stockée, pour toute la durée de leur conservation, de manière sécurisée. Les éléments obtenus dans le cadre d'un mandat et toutes les copies faites de ces éléments doivent être détruits dès qu'il n'existe plus de motifs pertinents de les conserver (voir l'article 150, paragraphes 2 et 5 et l'article 151, paragraphe 2, de l'IPA 2016). Il convient de noter que des garanties similaires, prévues dans le cadre juridique précédent (RIPA 2000), ont été jugées conformes aux exigences fixées par la Cour européenne des droits de l'homme pour le partage d'éléments obtenus par interception de masse avec des États étrangers ou des organisations internationales [Cour européenne des droits de l'homme (grande chambre), Big Brother Watch et autres/Royaume-Uni (voir note de bas de page 279 ci-dessus), points 362 et 399].

indépendante et judiciaire de l'utilisation des pouvoirs d'enquête en vertu de l'IPA 2016. L'IPC surveille l'utilisation des pouvoirs d'enquête prévus par l'IPA 2016 par les autorités répressives et les agences de sécurité nationale. La surveillance politique est assurée par la commission sur les services de renseignement du Parlement.

3.3.3.1 Surveillance au titre de la partie 4 de la loi sur la protection des données

(245) Le traitement des données à caractère personnel effectué par les services de renseignement au titre de la partie 4 de la DPA 2018 est surveillé par le commissaire à l'information[441].

(246) Les fonctions générales du commissaire à l'information en ce qui concerne le traitement de données à caractère personnel par des services de renseignement au titre de la partie 4 de la loi DPA 2018 sont énoncées à l'annexe 13 de la loi DPA 2018. Ses missions consistent notamment, sans s'y limiter, à contrôler et à faire appliquer la partie 4 de la DPA 2018, à favoriser la sensibilisation du public, à conseiller le Parlement, le gouvernement et d'autres institutions au sujet des mesures législatives et administratives, à encourager la sensibilisation des responsables du traitement et des sous-traitants en ce qui concerne les obligations qui leur incombent, à fournir des informations à une personne concernée sur l'exercice de ses droits, à effectuer des enquêtes, etc.

(247) S'agissant de la partie 3 de la DPA 2018, le commissaire dispose du pouvoir de notifier aux responsables du traitement une violation alléguée et d'émettre un avertissement lorsqu'un traitement est susceptible de violer les règles, puis d'émettre un rappel à l'ordre lorsque la violation est confirmée. Il peut également délivrer des avis d'exécution et de sanction en cas de violation de certaines dispositions de la loi[442]. Cependant, contrairement à ce qui est prévu pour d'autres parties de la DPA 2018, le commissaire ne peut pas adresser un avis d'évaluation à un organe de sécurité nationale[443].

(248) De plus, l'article 110 de la DPA 2018 prévoit une exception à l'utilisation de certains pouvoirs du commissaire lorsque cela est nécessaire pour garantir la sécurité nationale. Cette exception porte notamment sur le pouvoir du commissaire de délivrer des avis (de tout type) au titre de la loi sur la protection des données (avis d'information, d'évaluation, d'exécution et de sanction), sur le pouvoir de réaliser des inspections conformément aux obligations internationales, sur les pouvoirs d'accès et d'inspection

441 Article 116 de la DPA 2018.

442 Conformément à l'annexe 13, point 2, de la DPA 2018, des avis d'exécution et de sanction peuvent être adressés à un responsable du traitement ou à un sous-traitant en lien avec des violations du chapitre 2 de la partie 4 de la DPA 2018 (principes du traitement), d'une disposition de la partie 4 de la DPA 2018 conférant des droits à une personne concernée, d'une obligation de communiquer une violation de données à caractère personnel au commissaire au titre de l'article 108 de la DPA 2018 et des principes applicables aux transferts de données à caractère personnel vers des pays tiers, vers des pays n'ayant pas adhéré à la convention et à des organisations internationales au titre de l'article 109 de la DPA 2018 (pour de plus amples informations sur les avis d'exécution et de sanction, voir le considérant (92)).

443 En vertu de l'article 147, paragraphe 6, de la DPA 2018, le commissaire à l'information ne peut pas adresser un avis d'évaluation à un organe mentionné à l'article 23, paragraphe 3, de la loi de 2000 sur la liberté de l'information. Il peut notamment s'agir du *Security Service* (MI5), du *Secret Intelligence Service* (MI6) et du *Government Communications Headquarter* (GCHQ).

ainsi que sur les règles relatives aux infractions[444]. Comme expliqué dans le considérant (126), elle ne s'applique que si elle est nécessaire et proportionnée et au cas par cas.

(249) L'ICO et les services de renseignement britanniques ont signé un protocole d'accord[445] établissant un cadre pour la coopération sur un certain nombre de sujets, notamment la notification des violations de données et le traitement des réclamations des personnes concernées. Ce protocole prévoit notamment que, lorsqu'il reçoit une réclamation, l'ICO évalue si l'application d'une exemption concernant la sécurité nationale a été faite de manière appropriée. L'agence de renseignement concernée doit répondre aux questions posées par l'ICO dans le cadre de l'examen des réclamations individuelles dans un délai de 20 jours ouvrables, au moyen de canaux de communication sécurisés si des informations classifiées sont concernées. Depuis avril 2018 jusqu'à présent, l'ICO a reçu 21 réclamations introduites par des particuliers concernant les services de renseignement. Chaque réclamation a fait l'objet d'une évaluation et l'issue a été communiquée à la personne concernée[446].

3.3.3.2 Surveillance de l'utilisation des pouvoirs d'enquête au titre de l'IPA 2016

(250) Conformément à la partie 8 de l'IPA 2016, la surveillance de l'utilisation des pouvoirs d'enquête est assurée par le commissaire aux pouvoirs d'enquête (IPC). L'IPC est assisté par d'autres commissaires judiciaires, qui sont désignés collectivement sous le nom de commissaires judiciaires[447]. L'IPA 2016 définit les garanties qui protègent l'indépendance des commissaires judiciaires. Les commissaires judiciaires doivent exercer ou avoir exercé de hautes fonctions judiciaires (être ou avoir été membre des Cours supérieures)[448] et, comme tout membre du corps judiciaire, ils bénéficient d'un

444 Les dispositions pouvant faire l'objet d'une exemption sont les suivantes: l'article 108 (communication d'une violation de données à caractère personnel au commissaire); l'article 119 (inspection conformément aux obligations internationales); les articles 142 à 154 et l'annexe 15 (avis et pouvoirs d'accès et d'inspection du commissaire); et les articles 170 à 173 (infractions concernant des données à caractère personnel). De plus, concernant le traitement par les services de renseignement, l'annexe 13 (autres fonctions générales du commissaire), point 1, sous a) et g), et point 2.

445 Protocole d'accord entre le Bureau du commissaire à l'information et la communauté du renseignement britannique, voir la note de bas de page 165.

446 Dans le cas de sept réclamations, l'ICO a recommandé à l'auteur de la réclamation de signaler le problème au responsable du traitement (c'est le cas lorsqu'une personne a signalé le problème à l'ICO alors qu'elle aurait dû d'abord le signaler au responsable du traitement), dans le cas d'une réclamation, l'ICO a donné des conseils généraux au responsable du traitement (c'est le cas lorsque les actions du responsable du traitement ne semblent pas avoir violé la législation, mais que de meilleures pratiques auraient pu éviter que le problème ne soit signalé à l'ICO) et dans le cas des treize autres réclamations, le responsable du traitement n'a été tenu de prendre aucune mesure particulière (c'est le cas lorsque le problème signalé par la personne ne relève pas du champ d'application de la DPA 2018 car il concerne certes le traitement d'informations à caractère personnel, mais sur la base des informations fournies, le responsable du traitement ne semble pas avoir violé la législation).

447 Conformément à l'article 227, paragraphes 7 et 8, de l'IPA 2016, le commissaire aux pouvoirs d'enquête est un commissaire judiciaire et le commissaire aux pouvoirs d'enquête et les autres commissaires judiciaires sont désignés collectivement sous le nom de commissaires judiciaires. À l'heure actuelle, on compte 15 commissaires judiciaires.

448 Selon l'article 60, paragraphe 2, de la partie 3 de la loi de 2005 sur la réforme constitutionnelle, les «hautes fonctions judiciaires» correspondent aux fonctions de juge dans l'une des juridictions suivantes: i) la Cour suprême; ii) la Cour d'appel d'Angleterre et du pays de Galles (*Court of Appeal in England and Wales*); iii) la Haute Cour d'Angleterre et du pays de Galles (*High Court in England and Wales*); iv) la Cour de session (*Court of Session*); v) la Cour d'appel d'Irlande du Nord (*Court of Appeal in*

statut d'indépendance vis-à-vis du gouvernement[449]. Conformément à l'article 227 de l'IPA 2016, c'est le Premier ministre qui nomme l'IPC et autant de commissaires judiciaires qu'il le juge approprié. Tous les commissaires, qu'ils soient des membres actuels ou d'anciens membres du pouvoir judiciaire, ne peuvent être nommés que sur la base d'une recommandation commune des trois juges en chef pour l'Angleterre et le pays de Galles, l'Écosse et l'Irlande du Nord et du Lord Chancelier[450]. Le secrétaire d'État doit fournir à l'IPC du personnel, des locaux, des équipements et d'autres installations et services[451]. Le mandat des commissaires est de trois ans et peut être renouvelé[452]. Les commissaires judiciaires ne peuvent être destitués que dans des conditions strictes imposant un seuil élevé: soit par le Premier ministre, dans les circonstances spécifiques énumérées de manière exhaustive à l'article 228, paragraphe 5, de l'IPA 2016 (par exemple en cas de faillite ou d'emprisonnement), soit si une résolution approuvant cette destitution a été adoptée par les deux chambres du Parlement[453].

(251) Dans le cadre de leurs missions, l'IPC et les commissaires judiciaires sont assistés par le Bureau du commissaire aux pouvoirs d'enquête (IPCO). Le personnel de l'IPCO comprend une équipe d'inspecteurs, des experts juridiques et techniques internes et un comité consultatif sur les technologies, qui lui fournit des avis d'experts. Comme c'est le cas pour chaque commissaire judiciaire, l'indépendance de l'IPCO est protégée. L'IPCO est un organisme indépendant relevant du ministère de l'intérieur, c.-à-d. qu'il reçoit des financements de ce ministère mais qu'il exerce ses fonctions de manière indépendante[454].

(252) Les principales fonctions des commissaires judiciaires sont énoncées à l'article 229 de l'IPA 2016[455]. En particulier, les commissaires judiciaires disposent d'un large pouvoir d'approbation préalable, qui fait partie des garanties introduites dans le cadre

---

Northern Ireland); vi) la Haute Cour d'Irlande du Nord (*High Court in Northern Ireland*); ou aux fonctions de Lord judiciaire (*Lord of Appeal in Ordinary*).

449 L'indépendance des juges est établie par convention et a été largement reconnue depuis l'Acte d'établissement (*Act of Settlement*) de 1701.

450 Article 227, paragraphe 3, de l'IPA 2016. Les commissaires judiciaires doivent également être recommandés par le commissaire aux pouvoirs d'enquête, voir l'article 227, paragraphe 4, point e), de l'IPA 2016.

451 Article 238 de l'IPA 2016.

452 Article 227, paragraphe 2, de l'IPA 2016.

453 Le processus de destitution est identique au processus de destitution d'autres juges au Royaume-Uni (voir par exemple l'article 11, paragraphe 3, de la loi de 1981 sur les Cours supérieures et l'article 33 de la loi de 2005 sur la réforme constitutionnelle, qui exigent également une résolution suivie de l'approbation des deux chambres du Parlement). À ce jour, aucun commissaire judiciaire n'a été destitué.

454 Un organisme indépendant est une organisation ou une agence qui reçoit des financements d'un gouvernement, mais qui est en mesure d'agir de manière indépendante (pour une définition et de plus amples informations sur la notion d'organisme indépendant, voir le manuel du Bureau du Cabinet sur la classification des organismes publics, disponible à l'adresse suivante: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/519571/Classification-of-Public_Bodies-Guidance-for-Departments.pdf et le premier rapport de la session 2014-2015 de la commission spéciale de l'administration publique de la Chambre des communes, disponible à l'adresse suivante: https://publications.parliament.uk/pa/cm201415/cmselect/cmpubadm/110/110.pdf)

455 Conformément à l'article 229 de l'IPA 2016, les commissaires judiciaires disposent de pouvoirs de surveillance étendus qui couvrent également le contrôle de la conservation et de la divulgation des données collectées par les services de renseignement.

juridique du Royaume-Uni par l'IPA 2016. Les mandats portant sur l'interception ciblée, l'interférence avec des équipements, les ensembles de données à caractère personnel en masse, l'acquisition de masse de données de communication ainsi que les avis de conservation de données de communication doivent tous être approuvés par les commissaires judiciaires[456]. L'IPC doit également toujours autoriser au préalable l'acquisition de données de communication à des fins répressives[457]. Si un commissaire refuse d'approuver un mandat, le secrétaire d'État peut interjeter appel devant le commissaire aux pouvoirs d'enquête, dont la décision est définitive.

(253) Le rapporteur spécial de l'ONU sur le droit à la vie privée s'est vivement félicité de la création des commissaires judiciaires par l'IPA 2016 car «toutes les demandes de surveillance plus sensibles ou plus intrusives doivent être autorisées à la fois par un ministre du gouvernement et par le Bureau du commissaire aux pouvoirs d'enquête». Il a notamment souligné que «cet élément de contrôle juridictionnel [dans le cadre du rôle de l'IPC] soutenu par une équipe d'inspecteurs expérimentés et d'experts en technologie mieux dotée en ressources constitue l'une des nouvelles garanties les plus importantes introduites par l'IPA, qui a remplacé un ancien système fragmenté d'autorités de surveillance et complète le rôle de la commission sur le renseignement et la sécurité du Parlement et du tribunal chargé des pouvoirs d'enquête»[458].

(254) De plus, l'IPC dispose du pouvoir d'effectuer une surveillance ex post[459], y compris au moyen d'audits, d'inspections et d'enquêtes, de l'utilisation des pouvoirs d'enquête en vertu de l'IPA 2016 et d'autres pouvoirs et fonctions prévus par la législation en vigueur[460]. Les résultats de cette surveillance ex post figurent dans le rapport que l'IPC doit préparer chaque année et présenter au Premier ministre[461], et qui doit être publié et transmis au Parlement[462]. Le rapport contient des statistiques et des informations utiles concernant l'utilisation des pouvoirs d'enquête par les agences de renseignement et les autorités répressives et le déploiement des garanties relatives aux éléments couverts

456 Les décisions relatives à l'approbation d'une décision du secrétaire d'État de délivrer un mandat relèvent de la compétence des commissaires judiciaires eux-mêmes. Si un commissaire refuse d'approuver un mandat, le secrétaire d'État peut interjeter appel devant le commissaire aux pouvoirs d'enquête, dont la décision est définitive.

457 L'autorisation de l'IPC est toujours nécessaire lorsque les données de communication sont acquises à des fins répressives (article 60A de l'IPA 2016). Lorsque des données de communication sont acquises à des fins de sécurité nationale, l'autorisation peut être accordée par l'IPC ou par un haut fonctionnaire désigné de l'autorité publique compétente (voir les articles 61 et 61A de l'IPA 2016 et le considérant (203)).

458 Déclaration de fin de mission du rapporteur spécial sur le droit à la vie privée à l'issue de sa mission au Royaume-Uni de Grande-Bretagne et d'Irlande du Nord (voir la note de bas de page 281).

459 Article 229 de l'IPA 2016. Les pouvoirs d'enquête et d'information des commissaires judiciaires sont énoncés à l'article 235 de l'IPA 2016.

460 Il s'agit notamment des mesures de surveillance prévues au titre de la RIPA 2000, de l'exercice des fonctions au titre de la partie 3 de la loi de 1997 sur la police (autorisation d'agir concernant des biens) et de l'exercice par le secrétaire d'État de fonctions au titre des articles 5 à 7 de la loi de 1994 sur les services de renseignement [mandats d'interférence avec la télégraphie sans fil, d'accès et d'interférence avec des biens (article 229 de l'IPA 2016)].

461 Article 230 de l'IPA 2016. L'IPC peut également adresser de sa propre initiative au Premier ministre un rapport sur tout sujet relevant de ses fonctions. L'IPC doit également présenter un rapport au Premier ministre sur demande de celui-ci, et le Premier ministre peut demander à l'IPC d'examiner toute fonction des services de renseignement.

462 Certaines parties peuvent en être exclues dans le cas où leur publication serait contraire à la sécurité nationale.

par le secret professionnel, aux éléments journalistiques confidentiels et aux sources d'information journalistique, ainsi que des informations sur les dispositions prises et les finalités opérationnelles invoquées dans le cadre des mandats de masse. Enfin, le rapport annuel de l'IPCO précise les domaines dans lesquels des recommandations ont été adressées aux autorités publiques, ainsi que la manière dont elles ont été prises en compte[463].

(255) Conformément à l'article 231 de l'IPA 2016, si l'IPC prend connaissance de toute erreur importante commise par les autorités publiques dans le cadre de l'utilisation de leurs pouvoirs d'enquête, il doit en informer la personne concernée lorsqu'il considère que l'erreur est grave et qu'il est dans l'intérêt public d'informer la personne[464]. L'article 231 de l'IPA 2016 précise notamment que, lorsqu'il informe une personne de l'existence d'une erreur, l'IPC doit l'informer de son droit éventuel d'adresser une requête au tribunal chargé des pouvoirs d'enquête et lui fournir toutes les informations qu'il juge nécessaires à l'exercice de ce droit et dont la divulgation est dans l'intérêt public[465].

3.3.3.3 Surveillance parlementaire des services de renseignement

(256) La surveillance parlementaire assurée par la commission sur le renseignement et la sécurité (*Intelligence and Security Committee*, ISC) trouve son fondement juridique dans la loi de 2013 sur la justice et la sécurité (JSA 2013)[466]. Cette loi institue l'ISC en

---

463 Par exemple, dans le rapport annuel de 2019 de l'IPCO (point 6.38), il est mentionné qu'il a été recommandé au MI5 de modifier sa politique de conservation des ensembles de données à caractère personnel en masse (EDM) étant donné qu'il aurait dû adopter une approche tenant compte de la proportionnalité de la conservation pour tous les domaines des bases d'EDM et pour chaque EDM détenu. Fin 2018, l'IPCO n'était pas convaincu que cette recommandation avait été suivie et le rapport de 2019 a expliqué que le MI5 était en train de mettre en place une nouvelle procédure pour s'acquitter de cette obligation. Le rapport annuel de 2019 (point 8.22) mentionne également le fait qu'une série de recommandations a été adressée au GCHQ concernant son registre rendant compte de la proportionnalité de ses demandes relatives aux données en masse. Le rapport confirme que des progrès ont été accomplis dans ce domaine fin 2018. Rapport annuel de 2019 du Bureau du commissaire aux pouvoirs d'enquête, disponible à l'adresse suivante: https://www.ipco.org.uk/docs/IPC%20Annual%20Report%202019_Web%20Accessible%20version_final.pdf. En outre, chaque inspection de l'IPCO d'une autorité publique se conclut par un rapport qui est remis à l'autorité et qui contient des recommandations découlant de cette inspection. L'IPCO commence ensuite chaque inspection ultérieure par un examen des recommandations de la fois précédente et le nouveau rapport d'inspection précise si ces recommandations ont été suivies ou sont toujours pertinentes.

464 Une erreur est considérée comme «grave» lorsque le commissaire considère qu'elle a causé un préjudice ou un dommage considérable à la personne concernée (article 231, paragraphe 2, de l'IPA 2016). En 2018, 22 erreurs ont été signalées, dont huit ont été considérées comme graves et ont été portées à la connaissance de la personne concernée. Voir le rapport annuel de 2018 du Bureau du commissaire aux pouvoirs d'enquête, annexe C (voir https://www.ipco.org.uk/docs/IPCO%20Annual%20Report%202018%20final.pdf). En 2019, 14 erreurs ont été considérées comme graves. Voir le rapport annuel de 2019 du Bureau du commissaire aux pouvoirs d'enquête, annexe C, voir la note de bas de page 463.

465 L'article 231 de l'IPA 2016 précise que, lorsqu'il informe une personne de l'existence d'une erreur, l'IPC doit lui fournir les informations qu'il juge nécessaires à l'exercice de ces droits, en tenant particulièrement compte de la mesure dans laquelle la divulgation des informations serait contraire à l'intérêt public ou préjudiciable à la prévention ou la détection des infractions graves, la prospérité économique du Royaume-Uni ou la poursuite de l'exécution des missions des services de renseignement.

466 Comme l'ont expliqué les autorités britanniques, la loi sur la justice et la sécurité a développé le mandat de l'ISC pour y inclure un rôle de surveillance de la communauté du renseignement qui va au-delà des

tant que commission du Parlement britannique. Depuis 2013, les pouvoirs de l'ISC ont été renforcés et comprennent notamment la surveillance des activités opérationnelles des services de sécurité. Conformément à l'article 2 de la JSA 2013, l'ISC est chargé de surveiller les dépenses, la gestion, la politique et les opérations des agences de sécurité nationale. La JSA 2013 précise que l'ISC peut réaliser des enquêtes sur des questions opérationnelles lorsqu'elles ne portent pas sur des opérations en cours[467]. Le protocole d'accord conclu entre le Premier ministre et l'ISC[468] précise en détail les éléments à prendre en compte afin de déterminer si une activité relève ou non d'une opération en cours[469]. Le Premier ministre peut aussi demander à l'ISC d'enquêter sur des opérations en cours et l'ISC peut examiner les informations communiquées volontairement par les agences.

(257) En vertu de l'annexe 1 de la JSA 2013, l'ISC peut demander aux directeurs de l'un quelconque des trois services de renseignement de divulguer des informations. L'agence doit communiquer ces informations, sauf si le secrétaire d'État y oppose son veto[470]. Selon les explications fournies par les autorités britanniques, en pratique, très peu d'informations ne sont pas communiquées à l'ISC[471].

(258) L'ISC est composée de membres qui appartiennent à l'une des deux chambres du Parlement et sont nommés par le Premier ministre après consultation du dirigeant de l'opposition[472]. L'ISC doit présenter un rapport annuel au Parlement concernant l'exécution de ses missions et tout autre rapport qu'il juge nécessaire[473]. De plus, l'ISC est en droit de recevoir tous les trois mois la liste des finalités opérationnelles utilisées

---

trois agences de renseignement et permet la surveillance rétrospective des activités opérationnelles des agences sur des questions d'intérêt national majeur.

467 Article 2 de la JSA 2013.

468 Protocole d'accord entre le Premier ministre et l'ISC, disponible à l'adresse suivante: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf

469 Point 14 du protocole d'accord entre le premier ministre et l'ISC, voir la note de bas de page 468.

470 Le secrétaire d'État ne peut opposer son veto à la divulgation d'informations que pour deux raisons: les informations sont de nature sensible et ne devraient pas être divulguées à l'ISC dans l'intérêt de la sécurité nationale; ou les informations sont d'une nature telle que, si l'on demandait au secrétaire d'État de les présenter devant une commission spéciale de la Chambre des communes consacrée à un ministère donné, il considérerait (pour des raisons ne se limitant pas à la sécurité nationale) qu'il ne serait pas approprié de le faire. (Annexe 1, point 4 2), de la loi RIPA 2013).

471 Cadre explicatif relatif aux discussions sur l'adéquation du Royaume-Uni, section H: Sécurité nationale, page 43, voir la note de bas de page 31.

472 Article 1 de la JSA 2013. Les ministres ne sont pas éligibles au statut de membre. Les membres restent membres de l'ISC pour la durée du mandat parlementaire au cours duquel ils ont été nommés. Ils peuvent être destitués par une résolution de la Chambre qui les a nommés, s'ils cessent d'être parlementaires ou s'ils deviennent ministres. Un membre peut également démissionner.

473 Les rapports et déclarations de la commission sont disponibles en ligne à l'adresse suivante: https://isc.independent.gov.uk/publications/. En 2015, l'ISC a publié un rapport intitulé «Privacy and Security: a modern and transparent legal framework» (Vie privée et sécurité: un cadre juridique moderne et transparent) (voir: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf), dans lequel elle a analysé le cadre juridique applicable aux techniques de surveillance utilisées par les agences de renseignement et a publié une série de recommandations qui a été ensuite prise en compte et intégrée dans le projet de loi sur les pouvoirs d'enquête, devenu l'IPA 2016. La réponse du gouvernement au rapport sur la vie privée et la sécurité est disponible à l'adresse suivante: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf.

pour examiner les éléments obtenus en masse[474]. Le Premier ministre partage avec l'ISC des copies des enquêtes, des inspections ou des audits du commissaire aux pouvoirs d'enquête lorsque le sujet des rapports relève des compétences légales de la commission[475]. Enfin, la commission peut demander à l'IPC de réaliser une enquête et le commissaire doit informer l'ISC de sa décision de mener ou non cette enquête[476].

(259) L'ISC s'est également prononcée sur le projet de loi sur les pouvoirs d'enquête, ce qui a donné lieu à un certain nombre d'amendements qui ont été repris dans l'IPA 2016[477]. L'ISC a notamment recommandé de renforcer les protections de la vie privée en établissant une série de protections de la vie privée applicables à l'ensemble des pouvoirs d'enquête[478]. Elle a également suggéré de modifier les capacités envisagées concernant l'interférence avec des équipements, les EDM et les données de communication, et a demandé d'autres amendements spécifiques afin de renforcer les limitations et les garanties applicables à l'utilisation des pouvoirs d'enquête[479].

3.3.4 Recours

(260) Dans le domaine de l'accès des pouvoirs publics à des fins de sécurité nationale, les personnes concernées doivent disposer de la possibilité d'exercer des voies de droit devant un tribunal indépendant et impartial afin d'avoir accès à des données à caractère personnel les concernant, ou d'obtenir la rectification ou la suppression de telles données[480]. L'organe judiciaire en question doit notamment disposer du pouvoir d'adopter des décisions contraignantes pour les services de renseignement[481]. Au Royaume-Uni, comme l'expliquent les considérants (261) à (271), un certain nombre de voies de recours juridictionnel donnent aux personnes concernées la possibilité d'exercer de tels recours.

3.3.4.1 Mécanismes de recours possibles au titre de la partie 4 de la loi sur la protection des données

(261) En vertu de l'article 165 de la DPA 2018, une personne concernée a le droit d'introduire une réclamation auprès du commissaire à l'information si elle considère qu'une violation de la partie 4 de la DPA 2018 a été commise en lien avec des données à caractère personnel la concernant. Le commissaire à l'information a le pouvoir

474 Articles 142, 161 et 183 de l'IPA 2016.

475 Article 234 de l'IPA 2016.

476 Article 236 de l'IPA 2016.

477 Commission sur le renseignement et la sécurité du Parlement, rapport sur le projet de loi sur les pouvoirs d'enquête, disponible à l'adresse suivante: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20160209_ISC_Rpt_IPBillweb.pdf

478 Ces obligations générales relatives à la protection de la vie privée sont désormais énoncées à l'article 2, paragraphe 2, de l'IPA 2016, qui prévoit qu'une autorité publique agissant au titre de ladite loi doit déterminer si l'objectif visé par le mandat, l'autorisation ou l'avis pourrait être raisonnablement atteint par d'autres moyens moins intrusifs ou si le niveau de protection à appliquer 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 des informations en question, de l'intérêt public à assurer l'intégrité et la sécurité des systèmes de télécommunication et des services postaux et de tout autre aspect de l'intérêt public à assurer la protection de la vie privée.

479 Par exemple, à la suite de la demande de l'ISC, le nombre de jours pendant lesquels un mandat «urgent» peut être en vigueur avant que le commissaire judiciaire ne doive l'approuver a été réduit de cinq à trois jours ouvrables et l'ISC dispose désormais du droit de soumettre la question au commissaire aux pouvoirs d'enquête en vue d'une enquête.

480 Arrêt Schrems II, point 194.

481 Arrêt Schrems II, point 197.

d'évaluer le respect de la DPA 2018 par le responsable du traitement et le sous-traitant, et de les obliger à prendre les mesures nécessaires. De plus, en vertu de la partie 4 de la DPA 2018, les personnes ont le droit de s'adresser à la Haute Cour (ou à la Cour de session en Écosse) pour demander une ordonnance enjoignant au responsable du traitement de respecter le droit d'accès aux données[482], le droit de s'opposer au traitement[483], et le droit de rectification ou d'effacement[484].

(262) Les personnes peuvent également demander réparation du préjudice subi du fait d'une violation d'une exigence de la partie 4 de la DPA 2018 de la part du responsable du traitement ou d'un sous-traitant[485]. Les préjudices incluent tant les pertes financières que les préjudices n'entraînant pas de perte financière, comme les situations de détresse[486].

3.3.4.2 Mécanismes de recours possibles au titre de l'IPA 2016

(263) Les personnes physiques peuvent obtenir réparation en cas de violation de l'IPA 2016 auprès du tribunal chargé des pouvoirs d'enquête.

(264) Le tribunal chargé des pouvoirs d'enquête a été créé par la RIPA 2000 et est indépendant du pouvoir exécutif[487]. Conformément à l'article 65 de la RIPA 2000, les membres de ce tribunal sont nommés par Sa Majesté pour une durée de cinq ans. Un membre de ce tribunal peut être destitué par Sa Majesté à la suite d'une intervention[488] des deux chambres du Parlement[489].

(265) En vertu de l'article 65 de la RIPA 2000, le tribunal est l'organe judiciaire compétent pour entendre des plaintes des personnes lésées par une conduite mise en œuvre au titre de l'IPA 2016 ou de la RIPA 2000 ou par toute conduite des services de renseignement[490].

(266) Conformément à l'article 65 de la RIPA 2000, pour former un recours devant le tribunal chargé des pouvoirs d'enquête («condition pour se pourvoir en justice»), une personne doit être convaincue[491] du fait que la conduite d'un service de renseignement

---

482 Article 94, paragraphe 11, de la DPA 2018.

483 Article 99, paragraphe 4, de la DPA 2018.

484 Article 100, paragraphe 1, de la DPA 2018.

485 L'article 169 de la DPA 2018 autorise les réclamations introduites par «[u]ne personne qui a subi un préjudice du fait de la violation d'une exigence de la législation relative à la protection des données». Selon les informations fournies par les autorités britanniques, en pratique, il est probable qu'une réclamation ou une plainte à l'encontre des services de renseignement soit présentée auprès du tribunal chargé des pouvoirs d'enquête, qui dispose d'une vaste compétence, qui peut accorder des indemnisations/des dommages-intérêts et devant lequel le dépôt d'une réclamation n'entraîne aucun coût.

486 Article 169, paragraphe 5, de la DPA 2018.

487 Selon l'annexe 3 de la RIPA 2000, les membres doivent disposer d'une certaine expérience judiciaire et leur mandat peut être renouvelé.

488 Une «intervention» est une motion déposée devant le Parlement qui vise à informer le monarque des avis du Parlement sur une question spécifique.

489 Annexe 3, point 1 5), de la loi RIPA 2000.

490 Article 65, paragraphe 5, de la RIPA 2000.

491 Au sujet du critère de «conviction», voir l'affaire Human Rights Watch/Secretary of State [2016] UKIPTrib15_165-CH, point 41. Dans cette affaire, le tribunal chargé des pouvoirs d'enquête, en renvoyant à la jurisprudence de la Cour européenne des droits de l'homme, a conclu que le critère approprié consiste à déterminer si, en ce qui concerne la conviction affirmée qu'une conduite relevant de l'article 68, paragraphe 5, de la RIPA 2000 a été mise en œuvre par un service de renseignement ou pour le compte de celui-ci, cette conviction est fondée, par exemple parce que la personne peut se

a été mise en œuvre en lien avec elle, avec ses biens, avec les communications qu'elle a envoyées ou qui lui étaient adressées, ou avec son utilisation d'un service postal, d'un service de télécommunications ou d'un système de télécommunications[492]. De plus, l'auteur de la réclamation doit être convaincu du fait que la conduite a eu lieu dans des «circonstances contestables»[493] ou «qu'elle a été mise en œuvre par les services de renseignement ou pour leur compte»[494]. Étant donné que ce critère de «conviction» a été interprété de manière relativement large[495], les conditions pour se pourvoir en justice sont faibles.

(267) Lorsque le tribunal chargé des pouvoirs d'enquête examine une réclamation qui lui a été soumise, il doit déterminer si les personnes contre lesquelles les allégations sont portées dans la réclamation se sont intéressées à l'auteur de la réclamation, enquêter sur l'autorité accusée d'avoir commis les violations en question et établir si la conduite reprochée a eu lieu[496]. Lorsque ce tribunal procède à des audiences, il doit appliquer les mêmes principes de décision dans ces procédures que le ferait un tribunal pour une demande de contrôle juridictionnel[497]. De plus, les destinataires des mandats ou des

---

prétendre victime d'une violation causée par la simple existence de mesures de surveillance secrète ou d'une législation autorisant de telles mesures uniquement si elle est en mesure de démontrer que, du fait de sa situation personnelle, elle risque potentiellement d'être visée par ces mesures.

492 Article 65, paragraphe 4, point a), de la RIPA 2000.

493 Ces circonstances font référence à une conduite des autorités publiques mise en œuvre en vertu d'un pouvoir (par ex. un mandat, une autorisation/un avis d'acquisition de communications, etc.) ou aux cas dans lesquels les circonstances sont telles (que ce pouvoir existe ou non) qu'il aurait été inapproprié de mettre en œuvre cette conduite en l'absence de ce pouvoir, ou du moins sans avoir vérifié au préalable s'il convenait d'en faire la demande. Les conduites autorisées par un commissaire judiciaire sont considérées comme ayant été mises en œuvre dans des circonstances contestables (article 65, paragraphe 7ZA, de la RIPA 2000), tandis que d'autres conduites mises en œuvre avec l'autorisation d'une personne exerçant une fonction juridictionnelle ne sont pas considérées comme ayant été mises en œuvre dans des circonstances contestables (article 65, paragraphes 7 et 8, de la RIPA 2000).

494 Selon les informations fournies par les autorités britanniques, compte tenu du seuil peu élevé pour l'introduction d'une réclamation, il n'est pas inhabituel que l'enquête du tribunal détermine qu'en réalité, l'auteur de la réclamation n'a jamais fait l'objet d'une enquête menée par une autorité publique. Le dernier rapport statistique du tribunal chargé des pouvoirs d'enquête précise qu'en 2016, le tribunal a reçu 209 réclamations, dont 52 % ont été considérées comme fantaisistes ou vexatoires et 25 % ont débouché sur un non-lieu. Selon les explications fournies par les autorités britanniques, cela signifie soit qu'aucune activité/aucun pouvoir de surveillance secrète n'a été utilisé en lien avec l'auteur de la réclamation, soit que des techniques de surveillance secrète ont été utilisées, mais que le tribunal a considéré que l'activité était légale. De plus, 11 % ont été jugées comme ne relevant pas de la compétence du tribunal, ont été retirées ou invalidées, 5 % ont été jugées comme tombant sous le coup de la prescription et 7 % ont fait l'objet d'un jugement en faveur de l'auteur de la réclamation. Rapport statistique de 2016 du tribunal chargé des pouvoirs d'enquête, disponible à l'adresse suivante: https://www.ipt-uk.com/docs/IPT%20Statisical%20Report%202016.pdf.

495 Voir la décision dans l'affaire Human Rights Watch/Secretary of State [2016] UKIPTrib15_165-CH. Dans cette affaire, le tribunal chargé des pouvoirs d'enquête, en renvoyant à la jurisprudence de la Cour européenne des droits de l'homme, a conclu que le critère approprié, en ce qui concerne la conviction qu'une conduite relevant de l'article 68, paragraphe 5, de la RIPA 2000 a été mise en œuvre par un service de renseignement ou pour le compte de celui-ci, consiste à déterminer si cette conviction est fondée, notamment par le fait que la personne peut se prétendre victime d'une violation causée par la simple existence de mesures de surveillance secrète ou d'une législation autorisant de telles mesures uniquement si elle est en mesure de démontrer que, du fait de sa situation personnelle, elle risque potentiellement d'être visée par ces mesures (voir la décision dans l'affaire Human Rights Watch/Secretary of State, point 41).

496 Article 67, paragraphe 3, de la RIPA 2000.

497 Article 67, paragraphe 2, de la RIPA 2000.

avis au titre de l'IPA 2016 et toute autre personne exerçant des fonctions d'État, employée par les forces de police ou le commissariat en charge des enquêtes sur la police sont tenus de divulguer ou de fournir à ce tribunal tout document et information qu'il pourrait requérir afin de lui permettre d'exercer ses compétences[498].

(268) Le tribunal chargé des pouvoirs d'enquête doit informer l'auteur de la réclamation si une décision a été prise en sa faveur ou non[499]. Conformément à l'article 67, paragraphes 6 et 7, de la RIPA 2000, le tribunal peut rendre des ordonnances provisoires et accorder une indemnisation ou rendre toute autre décision qu'il juge appropriée. Il peut notamment s'agir d'une décision cassant ou annulant un mandat ou une autorisation ou d'une décision ordonnant la destruction de tout enregistrement des informations obtenues dans le cadre de l'exercice d'un pouvoir conféré par un mandat, une autorisation ou un avis ou détenues par une autorité publique concernant une personne[500]. Conformément à l'article 67A de la RIPA 2000, les décisions du tribunal peuvent faire l'objet d'un appel, à condition que le tribunal ou la cour d'appel compétente donne son autorisation.

(269) Enfin, il convient de noter que le rôle du tribunal chargé des pouvoirs d'enquête a fait l'objet de discussions dans le cadre des actions en justice portées devant la Cour européenne des droits de l'homme à plusieurs reprises, notamment dans l'affaire Kennedy/Royaume-Uni[501] et, plus récemment, dans l'affaire Big Brother Watch et autres/Royaume-Uni[502], dans laquelle la Cour a déclaré que «l'IPT offrait un recours juridictionnel solide à toute personne soupçonnant que ses communications avaient été interceptées par les services de renseignement»[503].

3.3.4.3 Autres mécanismes de recours possibles

(270) Comme l'expliquent les considérants (109) à (111), des voies de recours en vertu de la loi de 1998 sur les droits de l'homme et devant la Cour européenne des droits de l'homme[504] sont également disponibles dans le domaine de la sécurité nationale. L'article 65, paragraphe 2, de la RIPA 2000 donne au tribunal chargé des pouvoirs d'enquête une compétence exclusive pour toutes les réclamations introduites au titre

498 Article 68, paragraphes 6 et 7, de la RIPA 2000.

499 Article 68, paragraphe 4, de la RIPA 2000.

500 La décision rendue dans l'affaire Liberty & Others/the Security Service, SIS, GCHQ, [2015] UKIP Trib 13_77-H_2, constitue un exemple de l'application de ces pouvoirs. Le tribunal a tranché en faveur des deux auteurs de la réclamation car, dans un cas, les communications avaient été conservées au-delà des limites prévues et, dans l'autre, la procédure d'examen n'avait pas été respectée conformément au règlement intérieur du GCHQ. Dans la première affaire, le tribunal a ordonné aux services de renseignement de détruire les communications conservées plus longtemps que la période applicable. Dans la deuxième affaire, aucun ordre de destruction n'a été délivré puisque les communications n'avaient pas été conservées.

501 Arrêt dans l'affaire Kennedy, voir la note de bas de page 129.

502 Cour européenne des droits de l'homme, Big Brother Watch et autres/Royaume-Uni (voir note 268 ci-dessus), points 413 à 415.

503 Cour européenne des droits de l'homme, arrêt Big Brother Watch, point 425.

504 Comme l'illustre, par exemple, le récent arrêt de la grande chambre de la Cour européenne des droits de l'homme dans l'affaire Big Brother Watch et autres/Royaume-Uni (voir note 279 ci-dessus), cela permet un contrôle juridictionnel effectif – similaire à celui auquel sont soumis les États membres de l'Union – par une juridiction internationale sur le respect des droits fondamentaux par les autorités publiques lors de l'accès à des données à caractère personnel. En outre, l'exécution des arrêts de la Cour européenne des droits de l'homme est soumise à un contrôle spécifique du Conseil de l'Europe.

de la loi sur les droits de l'homme en lien avec les agences de renseignement[505]. Cela signifie, comme l'a fait observer la Haute Cour, que «la question de savoir s'il y a eu en l'espèce une violation de la loi sur les droits de l'homme ou non peut en principe être soulevée et tranchée par un tribunal indépendant qui peut avoir accès à tous les éléments pertinents, y compris à des informations confidentielles. […] Nous gardons également à l'esprit à cet égard le fait que le tribunal lui-même peut désormais faire l'objet d'un appel devant la juridiction de deuxième instance compétente (en Angleterre et au pays de Galles, il s'agirait de la Cour d'appel); et que la Cour suprême a récemment décidé que le tribunal est en principe soumis à un contrôle juridictionnel: voir l'arrêt dans l'affaire R (Privacy International)/Investigatory Powers Tribunal [2019] UKSC 22; [2019] 2 WLR 1219»[506].

(271) Il ressort de ce qui précède que lorsque les autorités répressives ou les autorités de sécurité nationale britanniques accèdent à des données à caractère personnel relevant du champ d'application de la présente décision, cet accès est régi par des lois qui définissent les conditions dans lesquelles il peut avoir lieu et qui garantissent que l'accès à ces données et leur utilisation ultérieure sont limités à ce qui est nécessaire et proportionné à l'objectif répressif ou de sécurité nationale poursuivi. De plus, cet accès est, dans la plupart des cas, soumis à l'autorisation préalable d'un organe judiciaire, au moyen de l'approbation d'un mandat ou d'une injonction de production, et fait dans tous les cas l'objet d'une surveillance indépendante. Une fois que les autorités publiques ont eu accès aux données, le traitement de celles-ci, y compris leur partage et leur transfert ultérieurs, est soumis à des garanties spécifiques en matière de protection des données en vertu de la partie 3 de la DPA 2018, qui correspondent aux garanties prévues par la directive (UE) 2016/680, en ce qui concerne le traitement par les autorités répressives, et en vertu de la partie 4 de la DPA 2018 en ce qui concerne le traitement par les agences de renseignement. Enfin, les personnes concernées bénéficient dans ce domaine de droits de recours administratifs et judiciaires effectifs et ont notamment le droit d'accéder aux données les concernant et d'obtenir la rectification ou l'effacement de telles données.

(272) Compte tenu de l'importance de ces conditions, limitations et garanties aux fins de la présente décision, la Commission suivra de près l'application et l'interprétation des règles britanniques régissant l'accès des pouvoirs publics aux données. Il s'agira notamment des évolutions législatives, de la réglementation et de la jurisprudence pertinentes, ainsi que des activités de l'ICO et d'autres autorités de surveillance dans ce domaine. Une attention particulière sera également accordée à l'exécution par le Royaume-Uni des arrêts pertinents de la Cour européenne des droits de l'homme, y compris les mesures recensées dans les «plans d'action» et les «rapports d'action» soumis au Comité des ministres dans le cadre du contrôle de la conformité avec les arrêts de la Cour.

4. CONCLUSION

(273) La Commission considère que le RGPD britannique et la DPA 2018 assurent 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.

---

505 Dans l'affaire Belhaj & others [2017] UKSC 3, la détermination de l'illégalité de l'interception d'éléments couverts par le secret professionnel était directement fondée sur l'article 8 de la CEDH (voir le moyen 11).

506 Haute Cour de Justice, arrêt Liberty, [2019] EWHC 2057 (Admin), point 170.

(274) 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 d'identifier et de sanctionner en pratique les infractions et offrent 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.

(275) 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, se limitera à ce qui est strictement nécessaire pour atteindre l'objectif légitime en question et qu'une protection juridictionnelle effective existe contre une telle ingérence.

(276) Dès lors, vu les constatations de la présente décision, il convient de décider que le Royaume-Uni garantit 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.

(277) Cette conclusion se fonde à la fois sur le régime national applicable du Royaume-Uni et sur ses engagements internationaux, notamment son adhésion à la convention européenne des droits de l'homme et 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.

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

(278) 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, annulés à la suite d'un recours en annulation ou déclarés invalides à la suite d'un renvoi préjudiciel ou d'une exception d'illégalité.

(279) 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 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.

(280) 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[507], 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

[507] Arrêt Schrems, point 65.

juridictions nationales, qui peuvent être tenues de procéder à un renvoi préjudiciel devant la Cour de justice[508].

6. SUIVI, SUSPENSION, ABROGATION OU MODIFICATION DE LA PRÉSENTE DÉCISION

(281) 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 après l'adoption de la présente décision afin de déterminer si ce pays continue d'assurer un niveau de protection essentiellement équivalent. Ce suivi est particulièrement important en l'espèce, car le Royaume-Uni gérera, appliquera et mettra en œuvre un nouveau régime de protection des données qui ne sera plus soumis au droit de l'Union et qui est susceptible d'évoluer. À cet égard, une attention particulière sera 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 présente décision; 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 l'ICO et par d'autres organismes indépendants alimenteront le suivi assuré par la Commission.

(282) 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 présente décision, ainsi que de toute évolution des pratiques relatives au traitement des données à caractère personnel évaluées dans 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 inclure l'évolution de la situation en ce qui concerne les éléments mentionnés au considérant (281).

(283) 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 de protection des données, en particulier en ce qui concerne les questions ou les plaintes de personnes concernées de l'UE au sujet du transfert de données à caractère personnel de l'Union à des responsables du traitement et des sous-traitants situés au Royaume-Uni. La Commission devrait également être informée de tout élément indiquant que les actions des autorités publiques britanniques responsables de la prévention, de la détection, des enquêtes et des poursuites en matière d'infractions pénales, ou de la sécurité nationale, y compris de tout organisme de surveillance, n'assurent pas le niveau de protection requis.

---

508 Arrêt Schrems, 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.»

(284) Si les informations disponibles, et notamment les informations issues du suivi de 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 britanniques compétentes et demander que des mesures appropriées soient prises dans un délai bien défini, qui ne peut dépasser trois mois. Si nécessaire, ce délai peut être prorogé pour une durée déterminée, compte tenu de la nature de la question en cause et/ou des mesures à prendre. Une telle procédure pourrait par exemple être déclenchée dans les cas où des transferts ultérieurs, notamment sur la base de nouveaux règlements d'adéquation adoptés par le secrétaire d'État ou d'accords internationaux conclus par le Royaume-Uni, ne seraient plus effectués en bénéficiant des garanties assurant la continuité de la protection au sens de l'article 44 du règlement (UE) 2016/679.

(285) 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.

(286) La Commission pourra également lancer cette procédure afin de modifier la 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.

(287) 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. DURÉE ET RENOUVELLEMENT DE LA PRÉSENTE DÉCISION

(288) La Commission doit tenir compte du fait que, à l'issue de la période de transition prévue par l'accord de retrait et dès que la disposition provisoire prévue par l'article 782 de l'accord de commerce et de coopération UE-Royaume-Uni cessera de s'appliquer, le Royaume-Uni gérera, appliquera et mettra en œuvre un nouveau régime de protection des données par rapport à celui qui était en place lorsqu'il était lié par le droit de l'Union. Cela pourra notamment donner lieu à des modifications ou à des changements concernant le cadre de protection des données évalué dans la présente décision, ainsi qu'à d'autres évolutions pertinentes.

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

(290) 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

(291) Le comité européen de la protection des données a publié son avis[509], dont il a été tenu compte dans l'élaboration de la présente décision.

(292) Les mesures prévues par la présente décision sont conformes à l'avis du comité institué en vertu de l'article 93 du règlement (UE) 2016/679,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

1. 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 du règlement (UE) 2016/679 de l'Union européenne vers le Royaume-Uni.

2. La présente décision 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 DPA 2018.

Article 2

Lorsque, afin de protéger les personnes à l'égard du traitement de leurs données à caractère personnel, les autorités de surveillance compétentes des États membres exercent les pouvoirs que leur confère l'article 58 du règlement (UE) 2016/679 concernant les transferts de données relevant du champ d'application défini à l'article 1er, l'État membre concerné en informe la Commission sans délai.

Article 3

3. La Commission suit de manière permanente l'application du cadre juridique sur lequel se fonde la présente décision, notamment les conditions dans lesquelles les transferts ultérieurs sont effectués, les droits individuels sont exercés et les autorités publiques britanniques ont accès aux données transférées sur la base de la présente décision, dans le but de déterminer si le Royaume-Uni continue d'assurer un niveau de protection adéquat au sens de l'article 1er.

4. Les États membres et la Commission s'informent mutuellement des cas dans lesquels le commissaire à l'information, ou toute autre autorité britannique compétente, échoue à faire respecter le cadre juridique sur lequel se fonde la présente décision.

5. Les États membres et la Commission s'informent mutuellement de tout élément indiquant que les atteintes au droit des personnes à la protection de leurs données à caractère personnel commises par des autorités publiques britanniques vont au-delà de ce qui est strictement nécessaire ou qu'il n'existe pas de protection juridique effective contre les atteintes de cette nature.

509 Avis 14/2021 concernant le projet de décision d'exécution de la Commission européenne conformément au règlement (UE) 2016/679 constatant le niveau de protection adéquat des données à caractère personnel assuré par le Royaume-Uni, disponible à l'adresse suivante: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-142021-regarding-european-commission-draft_en.

6. Lorsqu'elle est en possession d'éléments indiquant qu'un niveau de protection adéquat n'est plus assuré, la Commission en informe les autorités britanniques compétentes et peut suspendre, abroger ou modifier la présente décision.

7. La Commission peut suspendre, abroger ou modifier la présente décision si le défaut de coopération de la part des autorités britanniques l'empêche de déterminer si le constat établi à l'article 1er, paragraphe 1, est affecté.

Article 4

La présente décision expire 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.

Article 5

Les États membres sont destinataires de la présente décision.

Fait à Bruxelles, le 28.6.2021

Par la Commission
Didier REYNDERS
Membre de la Commission

AMPLIATION CERTIFIÉE CONFORME
Pour la Secrétaire générale

Martine DEPREZ
Directrice
Prise de décision & Collégialité
COMMISSION EUROPÉENNE