DÉCISION D'EXÉCUTION (UE) 2021/1773 DE LA COMMISSION

du 28 juin 2021

constatant, conformément à la directive (UE) 2016/680 du Parlement européen et du Conseil, le caractère adéquat du niveau de protection des données à caractère personnel assuré par le Royaume-Uni

[notifiée sous le numéro C(2021) 4801]

LA COMMISSION EUROPÉENNE,

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

vu la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil ([1]), et en particulier son article 36, paragraphe 3,

considérant ce qui suit:

1. INTRODUCTION

(1) La directive (UE) 2016/680 fixe les règles applicables au transfert des données à caractère personnel des autorités compétentes au sein de l'Union 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 par les autorités compétentes sont définies au chapitre V de la directive (UE) 2016/680, et plus précisément aux articles 35 à 40. Si le flux des données à caractère personnel en provenance ou à destination de pays non membres de l'Union européenne est essentiel à la coopération efficace en matière répressive, il convient de garantir que le niveau de protection des données à caractère personnel au sein de l'Union européenne n'est pas compromis par ces transferts ([2]).

(2) En vertu de l'article 36, paragraphe 3, de la directive (UE) 2016/680, la Commission peut constater au moyen d'un acte d'exécution qu'un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans un pays tiers en question, ou une organisation internationale, assurent 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 (sauf lorsqu'un autre État membre auprès duquel les données ont été collectées doit autoriser le transfert), comme prévu à l'article 35, paragraphe 1, et au considérant 66 de la directive (UE) 2016/680.

(3) Comme précisé à l'article 36, paragraphe 2, de la directive (UE) 2016/680, l'adoption d'une décision d'adéquation doit reposer sur une analyse approfondie de l'ordre juridique du pays tiers. Dans son évaluation, la Commission doit déterminer si le pays tiers en question assure un niveau de protection «essentiellement équivalent» à celui qui est assuré au sein de l'Union européenne [considérant 67 de la directive (UE) 2016/680]. La norme en fonction de laquelle le niveau «essentiellement équivalent» est évalué est celle établie par la législation de l'Union européenne, notamment la directive (UE) 2016/680, ainsi que par la jurisprudence de la Cour de justice de l'Union européenne ([3]). Les critères de référence pour l'adéquation définis par le 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 requis d'assurer 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 de niveau de protection adéquat 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 de la vie privée et leur mise en œuvre effective, leur opposabilité et le contrôle de leur application, le niveau requis de protection ([7]).

([1]) JO L 119 du 4.5.2016, p. 89.
([2]) Voir le considérant 64 de la directive (UE) 2016/680.
([3]) Voir, tout récemment, l'affaire C-311/18, Maximilian Schrems/Data Protection Commissioner (ci-après l'«arrêt Schrems II»), ECLI:EU:C:2020:559.
([4]) Voir les recommandations 01/2021 sur les critères de référence dans le cadre de la directive en matière de protection des données dans le domaine répressif, adoptées en février 2021, disponibles à l'adresse suivante: https://edpb.europa.eu/system/files/2021-05/recommendations012021onart.36led.pdf_fr.pdf.
([5]) Affaire C-362/14, Maximillian Schrems/Data Protection Commissioner (ci-après l'«arrêt Schrems»), ECLI:EU:C:2015:650, point 73.
([6]) Arrêt Schrems, point 74.
([7]) Communication de la Commission au Parlement européen et au Conseil intitulée «Échange et protection de données à caractère personnel à l'ère de la mondialisation», COM(2017) 7 du 10.1.2017, section 3.1, p. 6, disponible à l'adresse suivante: https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52017DC0007&from=FR.

(5) La Commission a soigneusement analysé la législation et les pratiques pertinentes du Royaume-Uni (UK). Sur la base de ses constatations, exposées ci-dessous, la Commission conclut que le Royaume-Uni assure un niveau de protection adéquat des données à caractère personnel transférées des autorités compétentes au sein de l'Union relevant du champ d'application de la directive (UE) 2016/680, vers les autorités compétentes au sein du Royaume-Uni relevant du champ d'application de la partie 3 de la loi de 2018 sur la protection des données (Data Protection Act 2018, la «loi DPA 2018») ([8]).

(6) La présente décision a pour effet d'autoriser ces transferts sans qu'il soit nécessaire d'obtenir une autre autorisation pendant une période de quatre ans, renouvelable, et sans préjudice des conditions exposées à l'article 35 de la directive (UE) 2016/680.

2. RÈGLES APPLICABLES AU TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL PAR LES AUTORITÉS COMPÉTENTES À DES FINS RÉPRESSIVES

2.1. Le cadre constitutionnel

(7) Le Royaume-Uni est une démocratie parlementaire. Il dispose d'un Parlement souverain qui constitue l'autorité suprême de toutes les autres institutions publiques, d'un pouvoir exécutif issu du Parlement et responsable devant ce dernier ainsi que d'un pouvoir judiciaire indépendant. Le pouvoir exécutif tire son autorité de sa capacité à bénéficier de la confiance de la Chambre des communes élue et il est responsable devant les deux Chambres du Parlement (Chambre des communes et Chambre des lords), qui sont elles-mêmes chargées de contrôler le gouvernement et de débattre des lois et de les adopter. Le Parlement du Royaume-Uni a délégué au Parlement écossais, au Parlement gallois (Sanedd Cymru) et à l'Assemblée d'Irlande du Nord la responsabilité de légiférer sur certaines questions internes en Écosse, au pays de Galles et en Irlande du Nord. Si la protection des données relève de la compétence exclusive du Parlement du Royaume-Uni, c'est-à-dire que la même législation s'applique dans tout le pays, d'autres domaines d'action politique présentant un intérêt pour la présente décision ont été décentralisés. Par exemple, les systèmes de justice pénale, y compris les fonctions de police (les activités exercées par les forces de police) en Écosse et en Irlande du Nord, sont respectivement dévolus au Parlement écossais et à l'Assemblée d'Irlande du Nord ([9]).

(8) Bien que le Royaume-Uni ne dispose pas d'une constitution codifiée à proprement parler, ses principes constitutionnels se sont dessinés au fil du temps, découlant notamment de la jurisprudence et de la convention. La valeur constitutionnelle de certains textes législatifs, tels que la Grande Charte (Magna Carta), la déclaration des droits de 1689 (Bill of Rights 1689) et la loi de 1998 sur les droits de l'homme (Human Rights Act 1998), a été reconnue. Les droits fondamentaux des personnes ont été intégrés dans ce corpus constitutionnel à partir de la common law, des textes législatifs et des traités internationaux, en particulier 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]).

(9) La loi de 1998 sur les droits de l'homme inscrit les droits énoncés dans la CEDH dans le droit du Royaume-Uni. Elle accorde à toute personne les droits et libertés fondamentaux prévus aux articles 2 à 12 et à l'article 14 de la CEDH et aux articles 1 à 3 du protocole n° 1 et à l'article 1er du protocole n° 13, lus en combinaison avec les articles 16 à 18 de la CEDH. Il s'agit notamment du droit au respect de la vie privée et familiale, qui inclut lui-même le droit à la protection des données, et du droit à un procès équitable ([11]). En particulier, en vertu de l'article 8 de la CEDH, il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit au respect de la vie privée que pour autant que cette ingérence est 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.

([8]) Loi de 2018 sur la protection des données, disponible à l'adresse suivante: https://www.legislation.gov.uk/ukpga/2018/12/contents.

([9]) Cadre explicatif du Royaume-Uni pour la discussion relative au niveau de protection adéquat, section F: Application des lois, disponible à l'adresse suivante: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

([10]) À l'origine, les principes de la convention n° 108 ont été mis en œuvre dans la loi du Royaume-Uni par l'intermédiaire de la loi de 1984 sur la protection des données, remplacée par la loi DPA 1998, puis par la loi DPA 2018 (lue conjointement avec le «RGPD du Royaume-Uni»). Le Royaume-Uni a en outre signé en 2018 le protocole d'amendement de la convention pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel (dite «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).

(10) Conformément à la loi de 1998 sur les droits de l'homme, toute action entreprise par les autorités publiques doit être compatible avec les droits garantis en vertu de la CEDH ([12]). En outre, les lois et règlements doivent être interprétés et appliqués d'une manière qui soit compatible avec ces droits ([13]). Dès lors qu'une personne estime que ses droits, y compris ses droits au respect de la vie privée et à la protection des données, ont été violés par les autorités publiques, cette personne peut obtenir réparation devant les juridictions du Royaume-Uni en application de la loi de 1998 sur les droits de l'homme et, en dernier ressort, après avoir épuisé toutes les voies de recours nationales, elle peut demander réparation devant la Cour européenne des droits de l'homme pour violation des droits garantis par la CEDH.

2.2. **Le cadre du Royaume-Uni relatif à la protection des données**

(11) Le Royaume-Uni s'est retiré de l'Union 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 relatif à la protection de données à caractère personnel au Royaume-Uni régissant le traitement de 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 des menaces pour la sécurité publique et la prévention de telles menaces, était constitué des parties pertinentes de la loi de 2018 sur la protection des données qui transposait la directive (UE) 2016/680.

(12) Afin de se préparer à la sortie de l'Union européenne, le gouvernement du Royaume-Uni a adopté la loi de 2018 sur l'Union européenne (retrait) ([15]), qui a inscrit la législation de l'Union directement applicable dans le droit du Royaume-Uni et a prévu que la législation nationale «dérivée du droit de l'Union européenne» reste applicable après la fin de la période de transition. Au titre de la loi de 2018 sur l'Union européenne (retrait), la partie 3 de la loi DPA 2018 ([16]) transposant la directive (UE) 2016/680 constitue une législation nationale «dérivée de l'Union européenne». En vertu de ladite loi, la législation nationale «dérivée de l'Union européenne» qui reste inchangée doit être interprétée par les juridictions du Royaume-Uni conformément à la jurisprudence pertinente de la Cour de justice de l'Union européenne (Cour de justice) et aux principes généraux du droit de l'Union, tels qu'ils étaient en vigueur juste avant la fin de la période de transition (dénommés respectivement «jurisprudence de l'Union européenne conservée» et «principes généraux du droit de l'Union européenne conservés») ([17]).

(13) En vertu de la loi de 2018 sur l'Union européenne (retrait), les ministres du Royaume-Uni sont habilités à arrêter des dispositions, par la voie de règlements, pour apporter les modifications nécessaires au droit de l'Union européenne conservé qui résultent du retrait du Royaume-Uni de l'Union. Les règlements de 2019 relatifs à la protection des données, à la vie privée et aux communications électroniques (amendements, etc.) (retrait de l'Union européenne) [Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (DPPEC Regulations)] ([18]) sont le fruit de l'exercice de ce pouvoir. Ils modifient la législation du Royaume-Uni sur la protection des données, notamment la loi DPA 2018, en vue de l'adapter au contexte national ([19]).

([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 («accord de retrait»), disponible à l'adresse suivante: https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=FR.

([15]) Loi de 2018 sur l'Union européenne (retrait), disponible à l'adresse suivante: https://www.legislation.gov.uk/ukpga/2018/16/contents.

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

([17]) Article 6 de la loi de 2018 sur l'Union européenne (retrait).

([18]) Les règlements de 2019 relatifs à la protection des données, à la vie privée et aux communications électroniques (amendements, etc.) (retrait de l'Union européenne) [Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019], disponibles à l'adresse suivante: https://www.legislation.gov.uk/uksi/2019/419/contents/made, tels que modifiés par les DPPEC 2020, disponibles à l'adresse suivante: https://www.legislation.gov.uk/ukdsi/2020/9780348213522.

([19]) Les règlements relatifs au retrait (Exit Regulations) apportent plusieurs modifications à la partie 3 de la loi DPA 2018. Un certain nombre de ces modifications sont d'ordre technique, comme la suppression des références à l'«État membre» ou à la «directive en matière de protection des données dans le domaine répressif» [voir, par exemple, l'article 48, paragraphe 8, ou l'article 73, paragraphe 5, point a), de la loi DPA 2018] au profit du «droit national», de manière que la partie 3 puisse effectivement opérer en tant que droit national après la fin de la période de transition. En certains endroits, d'autres types de modifications étaient nécessaires, par exemple en ce qui concerne «qui» adopte les «décisions d'adéquation» aux fins du cadre législatif du Royaume-Uni en matière de protection des données [voir l'article 74A de la loi DPA 2018], à savoir le secrétaire d'État au lieu de la Commission européenne.

(14) En conséquence, les normes juridiques relatives au traitement de 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 des menaces pour la sécurité publique et la prévention de telles menaces au Royaume-Uni après la fin de la période de transition en vertu de l'accord de retrait, continueront d'être énoncées dans les parties pertinentes de la loi DPA 2018, en particulier dans sa partie 3, mais telles que modifiées par les DPPEC. Le règlement général sur la protection des données du Royaume-Uni («RGPD du Royaume-Uni») ne s'applique pas à ce type de traitement.

(15) La partie 3 de la loi DPA 2018 prévoit les règles en matière de traitement de données à caractère personnel à des fins répressives, y compris les principes relatifs à la protection des données, les bases juridiques pour le traitement (licéité), les droits des personnes concernées, les obligations des autorités compétentes en tant que responsables du traitement et les limitations applicables aux transferts ultérieurs. Parallèlement, les parties 5 et 6 de la loi DPA 2018 prévoient des règles applicables en matière de supervision, d'application et de recours applicables au domaine répressif.

(16) En outre, compte tenu du rôle pertinent que jouent les forces de police dans le domaine répressif, il convient de porter une attention particulière aux règles régissant les fonctions de police. Les fonctions de police étant une compétence décentralisée, différents textes législatifs, qui sont toutefois similaires en ce qui concerne leur contenu, s'appliquent en la matière a) en Angleterre et au pays de Galles, b) en Écosse, et c) en Irlande du Nord ([20]). De plus, divers types de documents d'orientation apportent des précisions supplémentaires sur la manière dont les pouvoirs de police devraient être utilisés. Il existe trois grandes formes d'orientation pour les forces de police: 1) les orientations statutaires publiées en vertu de la législation, telles que le code de déontologie (Code of Ethics) ([21]) et le code de bonne pratique relatif à la gestion des informations policières (Code of Practice on the Management of Police Information, «CBP relatif à la gestion des informations policières») ([22]) publiés en vertu de la loi de 1996 sur la police (Police Act 1996) ([23]) ou les codes PACE ([24]) publiés en vertu de la loi sur la police et les preuves criminelles (Police and Criminal Evidence Act) ([25]), 2) la pratique professionnelle agréée pour la gestion des informations policières (orientations de la pratique professionnelle agréée pour la gestion des informations policières) [Authorised Professional Practice on the Management of Police Information (APP Guidance on the Management of Police Information)] ([26]), publiée par le collège des forces de police (College of Policing) et 3) les orientations opérationnelles (publiées par la police elle-même). Le Conseil national des chefs de la police (National Police Chiefs Council) (un organisme de coordination de toutes les forces de police du Royaume-Uni) publie des orientations opérationnelles que toutes les forces de police ont approuvées et qui s'appliquent donc au niveau national ([27]). Le but de ces orientations est de garantir une gestion des informations cohérente entre les forces de police ([28]).

(17) Le CBP relatif à la gestion des informations policières a été publié par le secrétaire d'État en 2005, en vertu des pouvoirs prévus par l'article 39A de la loi de 1996 sur la police ([29]). Tout code de bonne pratique publié au titre de la loi sur la police doit être approuvé par le secrétaire d'État et fait l'objet d'une consultation avec l'Agence nationale de lutte contre la criminalité avant sa présentation devant le Parlement. L'article 39A, paragraphe 7, de la loi sur la

([20]) Pour une explication plus détaillée sur les forces de police et leurs pouvoirs au Royaume-Uni, voir: Cadre explicatif du Royaume-Uni pour la discussion relative à l'adéquation, section F: Application des lois (voir la note de bas de page n° 9).

([21]) Code de bonne pratique pour les principes et normes de conduite professionnelle pour la profession policière en Angleterre et au pays de Galles (Code of Practice for the Principles and Standards of Professional Behaviour for the Policing Profession of England and Wales), disponible à l'adresse suivante: https://www.college.police.uk/What-we-do/Ethics/Documents/Code_of_Ethics.pdf; code de déontologie des services de police d'Irlande du Nord (Police Service Northern Ireland Code of Ethics), disponible à l'adresse suivante: https://www.nipolicingboard.org.uk/psni-code-ethics; code de déontologie pour les fonctions de police en Écosse (Code of Ethics for policing in Scotland), disponible à l'adresse suivante: https://www.scotland.police.uk/about-us/code-of-ethics-for-policing-in-scotland/.

([22]) Code de bonne pratique relatif à la gestion des informations policières, disponible à l'adresse suivante: http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf.

([23]) Loi de 1996 sur la police, disponible à l'adresse suivante: https://www.legislation.gov.uk/ukpga/1996/16/contents.

([24]) Codes de bonne pratique de la loi de 1984 sur la police et les preuves criminelles (PACE), disponibles à l'adresse suivante: https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-pace-codes-of-practice.

([25]) Loi de 1984 sur la police et les preuves criminelles, disponible à l'adresse suivante: https://www.legislation.gov.uk/ukpga/1984/60/contents.

([26]) Pratique professionnelle agréée pour la gestion des informations policières, disponible à l'adresse suivante: https://www.app.college.police.uk/app-content/information-management/management-of-police-information/.

([27]) Manuel de protection des données à l'intention des professionnels de la protection des données des forces de police (Data Protection Manual for Police Data Protection Professionals), disponible à l'adresse suivante: https://www.npcc.police.uk/2019%20FOI/IMORCC/225%2019%20NPCC%20DP%20Manual%20Draft%200.11%20Mar%202019.pdf.

([28]) Par exemple le CBP relatif à la gestion des informations policières (voir la note de bas de page n° 22) s'applique à la conservation d'informations relatives aux fonctions policières opérationnelles [voir le considérant 47 de la présente décision].

([29]) Selon les informations fournies par les autorités du Royaume-Uni, au cours des discussions sur l'adéquation, le collège des forces de police rédigeait un projet de code de bonne pratique pour la gestion des informations et des registres pour remplacer le CBP relatif à la gestion des informations policières. Ce projet de code a été publié pour consultation publique le 25 janvier 2021 et est disponible à l'adresse suivante: https://www.college.police.uk/article/information-records-management-consultation.

police exige que la police tienne dûment compte des codes publiés au titre de ladite loi, la police est donc tenue de les respecter ([30]). En outre, les orientations non statutaires (telles que les orientations de la pratique professionnelle agréée pour la gestion des informations policières) doivent toujours être cohérentes avec le CBP relatif à la gestion des informations policières, qui prévaut ([31]). En tout état de cause, bien qu'il puisse exister certaines situations opérationnelles dans lesquelles les agents de police doivent s'écarter de ces orientations, ils sont toujours tenus de se conformer aux exigences de la partie 3 de la loi DPA 2018 ([32]).

(18) Des orientations supplémentaires concernant la législation du Royaume-Uni sur la protection des données pour le traitement dans le domaine répressif sont fournies par le commissaire à l'information (Information Commissioner, «ICO») ([33]) (pour plus de détails sur l'ICO, voir les considérants 93 à 109). Bien qu'elles ne soient pas juridiquement contraignantes, les juridictions seraient tenues, dans le cadre d'une affaire portée devant une juridiction, de prendre en considération tout manquement aux orientations, puisque ces dernières revêtent une valeur interprétative et démontrent la manière dont le commissaire interprète et applique la législation sur la protection des données en pratique ([34]).

(19) Enfin, comme mentionné aux considérants 8 à 10, les autorités répressives du Royaume-Uni doivent garantir le respect de la CEDH et de la convention n° 108.

(20) Dans sa structure et ses principaux composants, le cadre juridique régissant le traitement des données par les autorités répressives en matière pénale du Royaume-Uni est donc très similaire 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. En conséquence, ces obligations découlant d'instruments internationaux juridiquement contraignants, notamment en ce qui concerne la protection des données à caractère personnel, constituent un élément particulièrement important du cadre juridique évalué dans la présente décision.

2.3. **Champ d'application matériel et territorial**

(21) Le champ d'application matériel de la partie 3 de la loi DPA 2018 coïncide avec le champ d'application de la directive (UE) 2016/680, tel que précisé à son article 2, paragraphe 2. La partie 3 s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, par une autorité compétente, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier par une autorité compétente.

(22) En outre, afin de relever du champ d'application de la partie 3, le responsable du traitement doit être une «autorité compétente» et le traitement doit être effectué «à des fins répressives». Par conséquent, le régime de protection des données évalué dans la présente décision s'applique à toutes les activités répressives de ces autorités compétentes.

(23) La notion d'«autorité compétente» est définie à l'article 30 de la loi DPA comme une personne figurant sur la liste établie à l'annexe 7 de la loi DPA 2018, ainsi que comme toute autre personne, dans la mesure où elle exerce des fonctions statutaires pour l'une des fins répressives. 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

([30]) Dans l'affaire R/Commissioner of Police of Metropolis [2014] EWCA Civ 585, le statut juridique du CBP relatif à la gestion des informations policières a été confirmé et le juge de la Chambre des lords (Lord Justice) Laws a déclaré qu'en vertu de l'article 39A de la loi de 1996 sur la police, le préfet de la police londonienne est tenu de respecter le CBP relatif à la gestion des informations policières et les orientations de la pratique professionnelle agréée pour la gestion des informations policières.

([31]) L'inspection de la police et des services d'incendie et de secours (Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services, «HMICFRS») inspecte les forces de police pour ce qui est de leur respect du CBP relatif à la gestion des informations policières.

([32]) Voir à cet égard l'avis du collège des forces de police en ce qui concerne le respect des orientations de la pratique professionnelle agréée pour tous les éléments des fonctions de police, qui explique que «[l]a pratique professionnelle agréée est approuvée par l'organisme professionnel des fonctions de police (collège des forces de police) en tant que source officielle de la pratique professionnelle en la matière. On attend des agents et du personnel de police qu'ils tiennent compte de la pratique professionnelle agréée dans l'exercice de leurs responsabilités. Il peut cependant y avoir des circonstances où il existe une raison opérationnelle légitime pour que les forces de police s'écartent de la pratique professionnelle agréée, à condition que cet écart soit clairement motivé. Il incomberait aux forces de police d'assumer la responsabilité de tout risque local et national associé au fait d'opérer en dehors des lignes directrices agréées au niveau national, et, si un incident ou une enquête a lieu en conséquence [par exemple par l'intermédiaire du Bureau indépendant sur la conduite policière (Independent Office of Police Conduct)], les forces de police sont tenues responsables de tout risque.», disponible à l'adresse suivante: https://www.app.college.police.uk/faq-page.

([33]) Guide relatif au traitement de données par les services répressifs (Guide to Law Enforcement Processing), disponible à l'adresse suivante: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/.

([34]) Voir l'affaire Bridges/the Chief Constable of South Wales Police [2019] EWHC 2341 (Admin) où, tout en notant la nature non statutaire des orientations du commissaire, la Haute Cour a déclaré que «[lorsqu'elle] évalue si un responsable du traitement des données s'est conformé ou non aux obligations de l'article 64 (obligation d'effectuer une analyse d'impact relative à la protection des données en ce qui concerne les traitements à haut risque), une juridiction tiendra compte des orientations publiées par le commissaire à l'information en matière d'analyses d'impact relatives à la protection des données».

Authority), l'Autorité de la concurrence et des marchés (Competition and Markets Authority), le Cadastre (Her Majesty's Land Register) ou l'Agence nationale de lutte contre la criminalité (National Crime Agency)], les agences chargées des poursuites, les autres agences de justice pénale et les autres titulaires ou organisations qui exercent des activités répressives ([35]). La partie 3 de la loi DPA 2018 s'applique également aux juridictions et aux tribunaux lorsque ces derniers exercent leurs fonctions juridictionnelles, à l'exception de la partie relative aux droits de la personne concernée et à la supervision effectuée par l'ICO ([36]). La liste des autorités compétentes établie à l'annexe 7 n'est pas définitive et est susceptible d'être mise à jour par le secrétaire d'État via des règlements prenant en considération les évolutions de l'organisation des fonctions publiques ([37]).

(24) Le traitement en question doit également être effectué «à des fins répressives», définies comme étant la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ([38]). Le traitement par une autorité compétente n'est pas régi par la partie 3 de la loi DPA 2018 lorsqu'il n'a pas lieu à des fins répressives. Tel sera le cas, par exemple, lorsque l'Autorité de la concurrence et des marchés enquête sur des affaires qui ne sont pas de nature criminelle (tels que les fusions d'entreprises). Dans ce cas, le RGPD du Royaume-Uni, ainsi que la partie 2 de la loi DPA 2018 s'appliqueront puisque le traitement de données à caractère personnel par les autorités compétentes est effectué à des fins autres que répressives. Afin de déterminer quel régime de protection des données s'applique (partie 3 ou 2 de la loi DPA 2018) au traitement de données à caractère personnel concerné, l'autorité compétente, à savoir le responsable du traitement, est tenue d'examiner si la «finalité principale» de ce traitement est l'une des fins répressives visées par la loi DPA 2018.

(25) En ce qui concerne le champ d'application territorial de la partie 3 de la loi DPA 2018, l'article 207, paragraphe 2, prévoit que le DPA s'applique au traitement de données à caractère personnel dans le cadre des activités d'une personne établie sur l'ensemble du territoire du Royaume-Uni. Cela comprend les autorités publiques des territoires d'Angleterre, du pays de Galles, d'Écosse et d'Irlande du Nord qui relèvent du champ d'application matériel de la partie 3 de la loi DPA 2018 ([39]).

2.3.1. *Définition des données à caractère personnel et de traitement*

(26) Les notions essentielles de données à caractère personnel et de traitement sont définies à l'article 3 de la loi DPA 2018 et s'appliquent à l'ensemble de la loi DPA. Les définitions suivent de près les définitions correspondantes énoncées à l'article 3 de la directive (UE) 2016/680. Aux termes de la loi DPA 2018, on entend par «données à caractère personnel» toute information se rapportant à une personne vivante identifiée ou identifiable ([40]). Conformément à l'article 3, paragraphe 3, de la loi DPA 2018, une personne est identifiable si elle peut être identifiée, directement ou indirectement, à partir des informations, y compris par référence à un nom ou un identifiant ou par référence à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. La notion de «traitement» est définie comme toute opération ou tout ensemble d'opérations appliquées à des informations ou des ensembles d'informations, telles que a) la collecte, l'enregistrement, l'organisation, la structuration ou la conservation; b) l'adaptation ou la modification; c) l'extraction, la consultation ou l'utilisation; d) la communication par transmission, la diffusion ou toute autre forme de mise à disposition; e) le rapprochement ou l'interconnexion; ou f) la limitation, l'effacement ou la destruction. En outre, le DPA définit le «traitement de données sensibles» comme «a) le traitement de données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les croyances religieuses ou philosophiques ou l'affiliation aux organisations syndicales; b) le traitement de données génétiques ou de données biométriques, dans le but d'identifier exclusivement une personne; c) le traitement de données concernant la santé; le traitement de données relatives à la vie ou l'orientation sexuelle d'une personne» ([41]). À cet égard, l'article 205 de la loi DPA 2018 fournit la définition de «données biométriques» ([42]), «données concernant la santé» ([43]) et «données génétiques» ([44]).

([35]) Parmi ces derniers, l'annexe 7 de la loi 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).

([36]) Article 43, paragraphe 3, de la loi DPA 2018.

([37]) Article 30, paragraphe 3, de la loi 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 communications (Government Communications Headquarters)] ne sont pas des autorités compétentes (voir l'article 30, paragraphe 2, de la loi DPA 2018) et la partie 3 de la loi DPA 2018 ne s'applique à aucune de leurs activités. Leurs activités relèvent du champ d'application de la partie 4 de la loi DPA 2018.

([38]) Article 31 de la loi DPA 2018.

([39]) Par conséquent, la loi DPA 2018 et, dès lors, la présente décision ne s'appliquent pas aux dépendances de la Couronne britannique ni aux autres territoires d'outre-mer du Royaume-Uni, tels que les Îles Falkland ou le territoire de Gibraltar.

([40]) Les données à caractère personnel relatives à une personne décédée ne relèvent pas du champ d'application de la loi DPA 2018.

([41]) Article 35, paragraphe 8, de la loi DPA 2018.

([42]) «Données biométriques»: les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques.

([43]) «Données concernant la santé»: les données à caractère personnel relatives à la santé physique ou mentale d'une personne, y compris la fourniture de soins de santé, qui révèlent des informations sur l'état de santé de cette personne.

([44]) «Données génétiques»: les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne qui donnent des informations uniques sur la physiologie ou l'état de santé de cet individu et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne en question.

(27) L'article 32 de la loi DPA 2018 précise les définitions de «responsable du traitement» et de «sous-traitant» dans le contexte du traitement de données à caractère personnel à des fins répressives, en suivant de près les définitions équivalentes de la directive (UE) 2016/680. Le responsable du traitement désigne l'autorité compétente qui détermine les finalités et les moyens du traitement de données à caractère personnel. Lorsque ce traitement est requis par la loi, le responsable du traitement est l'autorité compétente à laquelle cette obligation est imposée par ladite loi. Un sous-traitant est défini comme toute personne qui traite des données à caractère personnel pour le compte du responsable du traitement (autre qu'une personne qui est employée auprès du responsable du traitement).

2.4. **Garanties, droits et obligations**

2.4.1. *Licéité et loyauté du traitement*

(28) Conformément à l'article 35 de la loi DPA 2018, les données à caractère personnel doivent être traitées de manière licite et loyale, de façon similaire à ce qui est énoncé à l'article 4, paragraphe 1, point a), de la directive (UE) 2016/680. Conformément à l'article 35, paragraphe 2, de la loi DPA 2018, le traitement de données à caractère personnel pour l'une des fins répressives n'est licite que s'il est fondé sur la loi et que soit la personne concernée a donné son consentement au traitement à cette fin, soit le traitement est nécessaire à l'exécution d'une mission effectuée par une autorité compétente à cette fin.

2.4.1.1. Traitement sur la base du droit

(29) À l'instar de l'article 8 de la directive (UE) 2016/680, afin de garantir la licéité d'un traitement relevant de la partie 3 de la loi DPA 2018, ledit traitement doit être «fondé sur le droit». On entend par traitement «licite» tout traitement autorisé par un texte législatif, par la common law ou par des prérogatives royales ([45]).

(30) Les pouvoirs des autorités compétentes sont en général régis par des textes législatifs, ce qui signifie que leurs fonctions et leurs pouvoirs sont clairement fixés par les législations adoptées par le Parlement ([46]). Dans certains cas, la police ainsi que les autres autorités compétentes figurant sur la liste établie à l'annexe 7 de la loi DPA 2018 peuvent s'appuyer sur la common law pour traiter les données ([47]). La common law a évolué grâce à la jurisprudence établie par les décisions des juridictions. La common law est pertinente dans le contexte des pouvoirs dont dispose la police, qui tire de cette source de droit sa mission principale de protéger la population grâce à la détection et la prévention des infractions ([48]). Toutefois,

([45]) Point 181 des notes explicatives de la loi DPA 2018, disponibles à l'adresse suivante: https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf.

([46]) Par exemple, l'Agence nationale de lutte contre la criminalité tire ses pouvoirs de la loi de 2013 sur la criminalité et les tribunaux (Crime and Courts Act 2013), disponible à l'adresse suivante: https://www.legislation.gov.uk/ukpga/2013/22/contents. De la même manière, les pouvoirs de l'Agence sur les standards en matière de produits alimentaires (Food Standards Agency) sont prévus par la loi de 1999 sur les normes alimentaires (Food Standards Act 1999), disponible à l'adresse suivante: https://www.legislation.gov.uk/ukpga/1999/28/contents. D'autres exemples sont la loi de 1985 sur la poursuite des délinquants (Prosecution of Offenders Act 1985), qui a créé le ministère public (Crown Prosecution Service) (voir https://www.legislation.gov.uk/ukpga/1985/23/contents); la loi de 2005 sur les commissaires chargés des recettes et des douanes (Commissioners for Revenue and Customs Act 2005) qui a institué l'administration fiscale et douanière du Royaume-Uni (Her Majesty's Revenue and Customs) (voir: https://www.legislation.gov.uk/ukpga/2005/11/contents); la loi de 1995 sur les procédures pénales en Écosse [Criminal Procedure (Scotland) Act 1995], qui a institué la Commission écossaise de révision des affaires criminelles (Scottish Criminal Cases Review Commission) (voir: https://www.legislation.gov.uk/ukpga/1995/46/contents); la loi de 2002 sur la justice en Irlande du Nord [Justice (Northern Ireland) Act 2002], qui a mis en place le Parquet d'Irlande du Nord (Public Prosecution Service in Northern Ireland) (voir: https://www.legislation.gov.uk/ukpga/2002/26/contents), ainsi que la loi de 1987 sur la justice pénale (Criminal Justice Act 1987) qui a institué l'Office des fraudes graves (Serious Fraud Office) et lui a octroyé ses pouvoirs (voir: https://www.legislation.gov.uk/ukpga/1987/38/contents).

([47]) Par exemple, selon les informations communiquées par les autorités du Royaume-Uni, au sein du ministère public (Crown office and Procurator Fiscal Service), qui est chargé d'engager les poursuites en Écosse, le Lord Advocate (procureur général), qui est à la tête du système de poursuite écossais, tire de la common law son pouvoir d'enquêter sur les décès et de poursuivre les infractions, alors que certaines de ses fonctions sont établies par des textes législatifs. En outre, la Couronne et, par extension, divers gouvernements, départements et ministres tirent eux aussi leurs pouvoirs de la législation, de la common law et des prérogatives royales combinées (il s'agit de compétences de common law conférées à la Couronne mais exercées par les ministres).

([48]) Cadre explicatif du Royaume-Uni pour la discussion relative au niveau de protection adéquat, section F: Application des lois, page 8 (voir la note de bas de page n° 9).

les forces de police disposent de compétences prévues à la fois par la common law et par les textes législatifs ([49]) pour accomplir cette mission. Lorsque la police jouit d'une compétence prévue par les textes législatifs, celle-ci prévaut sur toute autre compétence de common law ([50]).

(31) L'étendue des compétences de common law d'un agent de police a été reconnue par les juridictions pour inclure «toutes les étapes qui lui semblent nécessaires au maintien de la paix, à la prévention des infractions ou à la protection des biens contre les actes criminels» ([51]). Les compétences de common law ne sont pas des compétences inconditionnelles. Elles sont soumises à une série de limitations, dont des limites fixées par les juridictions ([52]) et par la législation, notamment la loi de 1998 sur les droits de l'homme (Human Rights Act 1998) et la loi de 2010 sur l'égalité (Equality Act 2010) ([53]). En outre, pour les autorités compétentes qui traitent les données au titre de la partie 3 de la loi DPA 2018, cela comprend l'exercice des compétences de common law conformément aux exigences énoncées dans la loi DPA 2018 ([54]). De plus, toute décision d'effectuer un traitement de données, quel qu'il soit, doit tenir compte des exigences des orientations applicables, telles que le CBP relatif à la gestion des informations policières ou les orientations spécifiques à l'un des pays du Royaume-Uni ([55]). Un certain nombre de documents d'orientation sont publiés par le gouvernement et les services de police opérationnels pour garantir que les agents de police exercent leurs pouvoirs dans le cadre du traitement dans les limites établies par la common law ou les textes législatifs pertinents ([56]).

(32) Les prérogatives royales constituent une autre composante du «droit» et font référence à certains pouvoirs conférés à la Couronne et pouvant être exercés par l'exécutif, qui ne sont pas tirés du droit écrit, mais résultent de la souveraineté du monarque ([57]). Il existe très peu d'exemples de pouvoirs résultant de prérogatives pertinents dans le contexte répressif. Il s'agit, par exemple, du cadre d'assistance juridique mutuel, qui permet le partage de données par le secrétaire d'État avec des pays tiers à des fins répressives. Le pouvoir de partager les données de cette manière

([49]) Les textes législatifs majeurs prévoyant le régime des principaux pouvoirs de police (arrestations, perquisitions, autorisations pour le maintien en détention, prises d'empreintes digitales, prélèvements intimes, interceptions sur mandat, accès aux données de communication) sont: i) pour l'Angleterre et le pays de Galles, la loi de 1984 sur la police et les preuves criminelles (Police and Criminal Evidence Act 1984 – la loi PACE), disponible à l'adresse suivante: https://www.legislation.gov.uk/ukpga/1984/60/contents [telle que modifiée par la loi de 2012 sur la protection des libertés (Protection of Freedoms Act 2012 – la loi PoFA), disponible à l'adresse suivante: https://www.legislation.gov.uk/ukpga/2012/9/contents], et la loi de 2016 sur les pouvoirs d'enquête (Investigatory Powers Act 2016 – IPA), disponible à l'adresse suivante: https://www.legislation.gov.uk/ukpga/2016/25/contents), ii) pour l'Écosse, la loi de 2016 sur la justice pénale en Écosse [Criminal Justice (Scotland) Act 2016], disponible à l'adresse suivante: https://www.legislation.gov.uk/asp/2016/1/contents, et la loi de 1995 sur les procédures pénales en Écosse [Criminal Procedure (Scotland) Act 1995], disponible à l'adresse suivante: https://www.legislation.gov.uk/ukpga/1995/46/contents) iii) pour l'Irlande du Nord, l'ordonnance de 1989 sur la police et les preuves criminelles en Irlande du Nord [Police and Criminal Evidence (Northern Ireland) Order 1989], disponible à l'adresse suivante: https://www.legislation.gov.uk/nisi/1989/1341/contents.

([50]) Les autorités du Royaume-Uni ont expliqué que la primauté du droit écrit est établie de longue date au Royaume-Uni, à savoir depuis l'arrêt dans l'affaire Entick/Carrington [1765] EWHC KB J98, qui reconnaissait l'existence de limites à l'exercice des pouvoirs par l'exécutif et arrêtait le principe selon lequel les compétences de common law et les pouvoirs résultant des prérogatives du monarque et du gouvernement sont subordonnés aux lois du pays.

([51]) Voir l'affaire Rice/Connolly [1966] 2 QB 414.

([52]) Voir l'affaire R(Catt)/Association of Chief police Officers [2015] AC 1065, dans laquelle, en ce qui concerne les pouvoirs de police pour obtenir et conserver les informations relatives à une personne (qui a commis une infraction), Lord Sumption a estimé que, au titre de la common law, la police a le pouvoir d'obtenir et de conserver des informations à des fins policières, c'est-à-dire, au sens large, pour le maintien de l'ordre public et pour la prévention et la détection des infractions. Ces pouvoirs n'autorisent pas les méthodes intrusives pour l'obtention d'informations, telles que la violation de propriété privée ou les actes (autres que l'arrestation en vertu des compétences de common law) qui constitueraient une agression. Dans cette affaire, le juge a estimé que les compétences de common law suffisaient largement pour autoriser l'obtention et la conservation du type d'informations publiques en question dans ces recours.

([53]) Loi de 2010 sur l'égalité, disponible à l'adresse suivante: https://www.legislation.gov.uk/ukpga/2010/15/contents.

([54]) Pour un exemple d'affaire dans laquelle les compétences de common law sont évaluées dans le cadre de la loi DPA 1998, voir la décision de la Haute Cour dans l'affaire Bridges/the Chief Constable of South Wales Police (voir la note de bas de page n° 33). Voir également les affaires Vidal-Hall/Google Inc. [2015] EWCA Civ 311 et Richard/BBC [2018] EWHC 1837 (Ch).

([55]) Voir, par exemple, les orientations du Service de police d'Irlande du Nord (Police Service of Northern Ireland) sur les prescriptions de service en matière de gestion des registres, disponibles à l'adresse suivante: https://www.psni.police.uk/globalassets/advice–information/our-publications/policies-and-service-procedures/records-management-080819.pdf.

([56]) La Chambre des communes a publié un document d'information qui fixe les compétences essentielles prévues par la common law et par les textes législatifs de la police en Angleterre et au pays de Galles (voir: https://researchbriefings.files.uk/documents/CBP-8637/CBP-8637.pdf). Par exemple, d'après ce document, si les pouvoirs de maintien de la «paix de la Couronne» sont des compétences dérivées de la common law, de même que le «recours à la force», «les pouvoirs d'interpellation et de fouille» découlent toujours du droit écrit. En outre, le gouvernement écossais publie sur son site web des informations relatives aux pouvoirs d'arrestation et d'interpellation et de fouille de la police (voir: https://www.gov.scot/policies/police/police-powers).

([57]) Selon les informations communiquées par les autorités du Royaume-Uni, les pouvoirs résultant des prérogatives exercés par le gouvernement comprennent, par exemple, l'élaboration et la ratification de traités, la conduite de la diplomatie et le recours aux forces armées au Royaume-Uni pour soutenir la police dans le maintien de la paix.

n'est pas toujours établi dans le droit écrit ([58]). Les prérogatives royales sont liées par les principes de la common law ([59]) et subordonnées au droit écrit et, en conséquence, sont soumises aux limites fixées par la loi de 1998 sur les droits de l'homme et par la loi DPA 2018 ([60]).

(33) À l'instar de l'article 8 de la directive (UE) 2016/680, le régime du Royaume-Uni exige que, en vue de respecter le principe de licéité, les autorités compétentes veillent à ce que, lorsque le traitement est fondé sur le droit, il soit également «nécessaire» à l'exécution d'une mission effectuée à des fins répressives. L'ICO fournit des orientations sur le sujet, précisant que le traitement «doit être un moyen ciblé et proportionné d'atteindre la finalité. La base juridique ne s'appliquera pas si la finalité peut être raisonnablement atteinte grâce à d'autres moyens moins intrusifs. Soutenir que le traitement est nécessaire parce que vous avez choisi de gérer votre entreprise d'une manière spécifique ne suffit pas. La question est de savoir si le traitement est nécessaire à la finalité exposée» ([61]).

2.4.1.2. Traitement fondé sur le «consentement» de la personne concernée

(34) Comme mentionné au considérant 28, l'article 35, paragraphe 2, de la loi DPA 2018 prévoit la possibilité d'effectuer le traitement des données à caractère personnel sur la base du «consentement» de la personne.

(35) Cependant, le consentement ne semble pas constituer une base juridique pertinente pour les opérations de traitement relevant du champ d'application de la présente décision. En réalité, les opérations de traitement couvertes par la présente décision concerneront toujours les données transférées par une autorité compétente d'un État membre vers une autorité compétente du Royaume-Uni au titre de la directive (UE) 2016/680. Par conséquent, elles n'impliqueront généralement pas le type d'interaction directe (collecte) entre une autorité publique et les personnes concernées, qui peut être fondé sur le consentement en vertu de l'article 35, paragraphe 2, point a), de la loi DPA 2018.

(36) Bien que le recours au consentement ne soit donc pas considéré comme pertinent pour l'évaluation menée dans le cadre de la présente décision, il convient de noter, par souci d'exhaustivité, que dans un contexte répressif le traitement n'est jamais fondé sur le consentement seul, puisqu'une autorité compétente doit toujours disposer d'un pouvoir sous-jacent qui lui permet de traiter les données ([62]). Plus précisément, à l'instar de ce qui est autorisé en vertu de la directive (UE) 2016/680 ([63]), cela signifie que le consentement fait office de condition supplémentaire pour permettre certaines opérations de traitement limitées et spécifiques qui pourraient autrement ne pas être effectuées, par exemple, la collecte et le traitement d'un échantillon ADN d'une personne qui n'est pas suspectée. Dans ce cas, si le consentement n'était pas donné ou était retiré, le traitement ne serait pas effectué ([64]).

([58]) À cet égard, voir l'évaluation du régime des transferts ultérieurs du Royaume-Uni aux considérants 74 à 87.

([59]) Voir l'affaire Bancoult/Secretary of State for Foreign and Commonwealth Affairs [2008] UKHL 61, dans laquelle les juridictions ont estimé que le pouvoir d'adopter des décrets en conseil, qui résulte des prérogatives, était également soumis aux motifs ordinaires du contrôle juridictionnel.

([60]) Voir l'affaire Attorney-General/De Keyser's Royal Hotel Ltd [1920] AC 508, dans laquelle la juridiction a jugé que les pouvoirs résultant des prérogatives ne peuvent être exercés lorsque les pouvoirs découlant des textes législatifs les remplacent; l'affaire Laker Airways/Department of Trade [1977] QB 643, dans laquelle la juridiction a estimé que les pouvoirs résultant des prérogatives ne peuvent être utilisés dans le but d'entraver le droit écrit; l'affaire R/Secretary of State for the Home Department, ex parte Fire Brigades Union [1995] UKHL 3, dans laquelle la juridiction a jugé que les pouvoirs résultant des prérogatives ne peuvent être exercés lorsqu'ils rentrent en contradiction avec la législation promulguée, même si cette dernière n'est pas encore en vigueur; l'affaire R (Miller)/ Secretary of State for Exiting the European Union [2017] UKSC 5, dans laquelle la juridiction a confirmé la capacité du droit écrit à adapter et abroger les pouvoirs résultant des prérogatives. Pour un aperçu général de la relation entre les prérogatives royales et les compétences résultant du droit écrit ou de la common law, voir le document d'information de la Chambre des communes, disponible à l'adresse suivante: https://researchbriefings.files.parliament.uk/documents/SN03861/SN03861.pdf.

([61]) Guide relatif au traitement de données par les services répressifs, «Sur quoi porte le premier principe?» («What is the first principle about?»), disponible à l'adresse suivante: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/#ib2.

([62]) Cela découle du libellé de la disposition pertinente de la loi DPA 2018, selon laquelle le traitement de données à caractère personnel pour l'une des fins répressives n'est licite que si, et dans la mesure où, il est «fondé sur le droit» et: soit a) la personne concernée a donné son consentement au traitement à cette fin, soit b) le traitement est nécessaire à l'exécution d'une mission effectuée par une autorité compétente à cette fin.

([63]) Voir les considérants 35 et 37 de la directive (UE) 2016/680.

([64]) Les autorités du Royaume-Uni ont expliqué, à titre d'exemple, qu'un cas dans lequel le consentement pourrait être une base adéquate pour le traitement serait celui où la police obtient un échantillon ADN d'une personne disparue dans le but de le comparer à l'ADN d'un corps éventuellement trouvé. Dans de telles circonstances, il serait inadéquat que la police oblige la personne concernée à fournir un échantillon; au lieu de cela, la police demanderait le consentement de la personne, qui est donné librement et peut être retiré à tout moment. Si le consentement venait à être retiré, les données ne pourraient plus être traitées, sauf si une nouvelle base juridique était établie pour continuer à traiter l'échantillon (par exemple, la personne concernée est devenue suspecte). Un autre exemple pourrait se présenter si les forces de police enquêtent sur une infraction dont la victime (qui pourrait être la victime d'un vol avec violence, d'une infraction à caractère sexuel, de violence domestique, ou être un proche d'une victime d'homicide ou d'une autre victime d'une infraction) pourrait bénéficier d'un renvoi vers Victim Support (Aide aux victimes – une organisation caritative indépendante qui œuvre à soutenir les personnes touchées par la criminalité et les événements traumatiques). Dans de telles circonstances, la police ne partagera les données à caractère personnel telles que le nom et les coordonnées avec Victim Support que si elle a obtenu le consentement de la victime.

(37) Dans les cas qui nécessitent le consentement de la personne, ce dernier doit être sans équivoque et impliquer une action affirmative claire ([65]). Les forces de police sont tenues de disposer d'une déclaration de protection des données comprenant, entre autres, les informations requises concernant l'utilisation valable du consentement. De plus, certaines forces de police publient de la documentation supplémentaire sur la façon dont elles se conforment à la législation sur la protection des données, et notamment comment et quand elles utilisent le consentement comme base juridique ([66]).

2.4.1.3. Traitement de données sensibles

(38) Des garanties spécifiques devraient être prévues pour le traitement des «catégories particulières» de données. À cet égard, à l'instar de l'article 10 de la directive (UE) 2016/680, la partie 3 de la loi DPA 2018 prévoit des garanties renforcées pour le traitement des données dites «sensibles» ([67]).

(39) Conformément à l'article 35, paragraphe 3, de la loi DPA 1998, les données sensibles peuvent être traitées par les autorités compétentes à des fins répressives dans deux cas uniquement: 1) la personne concernée a donné son consentement au traitement à des fins répressives et, au moment où le traitement est effectué, le responsable du traitement dispose d'un document stratégique approprié ([68]); ou 2) le traitement est strictement nécessaire aux fins répressives, il remplit au moins une des conditions énoncées à l'annexe 8 de la loi DPA 2018 et, au moment où le traitement est effectué, le responsable du traitement dispose d'un document stratégique approprié ([69]).

(40) En ce qui concerne le premier cas et comme expliqué au considérant 38, le recours au consentement n'est pas considéré comme pertinent pour le type de situation de transfert faisant l'objet de la présente décision ([70]).

(41) Lorsque le traitement de données sensibles ne repose pas sur le consentement, il peut être effectué en invoquant une des conditions énumérées à l'annexe 8 de la loi DPA 2018. Ces conditions portent sur le traitement nécessaire à des fins légales; à l'administration de la justice; à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne; à la protection des enfants et des personnes à risque; aux actions en justice; aux actes judiciaires; à la prévention de la fraude; à l'archivage; lorsque les données à caractère personnel sont manifestement rendues publiques par la personne concernée. À l'exception du cas où les données sont manifestement rendues publiques,

([65]) Il n'existe aucune définition distincte de «consentement» aux fins du traitement de données à caractère personnel visées à la partie 3 de la loi DPA 2018. L'ICO a fourni des orientations sur la notion de «consentement» dans la partie 3 de la loi DPA 2018, précisant qu'elle revêtait la même signification et devait être alignée sur la définition énoncée dans le RGPD, notamment que «le consentement doit être donné de façon libre, spécifique et éclairée et [qu']il doit y avoir un véritable choix quant à l'accord au traitement des données» [guide relatif au traitement de données par les services répressifs, «Sur quoi porte le premier principe?» (voir la note de bas de page n° 64) et le guide sur la protection des données, «Consentement» (*Guide to Data Protection*, «*Consent*»), disponible à l'adresse suivante: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/).

([66]) Voir, par exemple, les informations publiées sur la page web de la police du comté Lincolnshire (voir: https://www.lincs.police.uk/resource-library/data-protection/law-enforcement-processing/) ou sur la page web de la police du comté West Yorkshire (voir: https://www.westyorkshire.police.uk/sites/default/files/2018-06/data_protection.pdf).

([67]) Article 35, paragraphe 8, de la loi DPA 2018.

([68]) Article 35, paragraphe 4, de la loi DPA 2018.

([69]) Article 35, paragraphe 5, de la loi DPA 2018.

([70]) Par souci d'exhaustivité, il convient de noter que, lorsque le traitement repose sur le consentement, ce dernier doit être donné de façon libre, spécifique et éclairée et il doit y avoir un véritable choix quant à l'accord au traitement des données. En outre, lorsqu'il procède au traitement sur la base du consentement de la personne concernée, le responsable du traitement est tenu de disposer d'un «document stratégique approprié». L'article 42 de la loi DPA 2018 énonce les exigences que ce document doit satisfaire. Il précise que ce document doit, au minimum, expliquer les procédures du responsable du traitement pour garantir le respect des principes de protection des données, ainsi que les politiques dudit responsable en matière de conservation et d'effacement des données à caractère personnel. Conformément à l'article 42 de la loi DPA 2018, cela signifie que le responsable du traitement doit élaborer un document a) qui explique les procédures dudit responsable pour garantir le respect des principes de protection des données; et b) qui explique les politiques dudit responsable en matière de conservation et d'effacement des données à caractère personnel traitées sur la base du consentement de la personne concernée ou qui précisent la durée probable de conservation desdites données. En particulier, le document stratégique exige que le responsable du traitement, dans le respect de sa mission d'enregistrement des activités de traitement, inclue toujours les éléments mentionnés aux points a) et b). L'ICO a publié un modèle de document [guide relatif au traitement de données par les services répressifs: «Conditions pour le traitement de données sensibles» («*Conditions for sensitive processing*»), disponible à l'adresse suivante: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/conditions-for-sensitive-processing] et peut prendre des mesures répressives si les responsables du traitement manquent à ces exigences. Les juridictions étudient également le document stratégique approprié lorsque d'éventuelles violations de la loi DPA 2018 sont examinées. Par exemple, dans la récente affaire R (Bridges)/Chief Constable of South Wales Police, les juridictions ont examiné le document stratégique approprié du responsable du traitement et jugé que ce dernier était certes approprié, mais qu'il aurait gagné à être plus de précis. En conséquence, la police du pays de Galles du Sud a évalué et mis à jour le document stratégique approprié conformément aux nouvelles orientations de l'ICO (voir la note de bas de page n° 33). Par ailleurs, en vertu de l'article 42, paragraphe 3, de la loi DPA 2018, le responsable du traitement devrait régulièrement réviser le document stratégique approprié. Enfin, à titre de garantie supplémentaire, le responsable du traitement doit, en application de l'article 42, paragraphe 4, de la loi DPA 2018, tenir un registre consolidé des activités de traitement comprenant des éléments additionnels par rapport à l'obligation générale, qui incombe au responsable du traitement et qui est énoncée à l'article 61 de la loi DPA 2018, de tenir des registres relatifs aux activités de traitement.

toutes les conditions prévues par l'annexe 8 sont soumises à un contrôle du critère de «stricte nécessité». Comme précisé par l'ICO, «dans ce contexte, strictement nécessaire signifie que le traitement doit être lié à un besoin social impérieux, auquel on ne peut raisonnablement subvenir grâce à d'autres moyens moins intrusifs» ([71]). En outre, certaines des conditions sont soumises à d'autres limitations. À titre d'exemple, un critère supplémentaire d'intérêt public substantiel doit être rempli pour invoquer la condition de «fins légales» et la «condition de protection» (points 1 et 4 de l'annexe 8). De plus, en ce qui concerne les conditions relatives à la protection de l'enfant (point 4 de l'annexe 8), la personne concernée doit également avoir un âge déterminé et être considérée comme une personne à risque. Par ailleurs, le responsable du traitement ne peut faire valoir la condition prévue au point 4 de l'annexe 8 que dans des circonstances particulières ([72]). De la même manière, des limitations s'appliquent aux conditions relatives aux «actes judiciaires» et à la «prévention de la fraude» (points 7 et 8 de l'annexe 8 respectivement). Les deux ne s'appliquent qu'à des responsables du traitement spécifiques. Dans le cas des actes judiciaires, seule une juridiction ou une autre autorité judiciaire peut faire valoir cette condition, et dans le cas de la prévention de la fraude, seuls les responsables du traitement qui sont des organisations de lutte contre la fraude peuvent invoquer cette condition.

(42) Enfin, lorsque le traitement repose sur l'une des conditions figurant sur la liste établie à l'annexe 8, et en vertu de l'article 42 de la loi DPA 2018 respectivement, un «document stratégique approprié» doit être en place – expliquant les procédures du responsable du traitement pour garantir le respect des principes de protection des données, ainsi que les politiques dudit responsable en matière de conservation et d'effacement des données à caractère personnel – et des obligations de tenir un registre consolidé s'appliquent.

2.4.2. *Limitation de la finalité*

(43) Les données à caractère personnel devraient être traitées dans un but précis et être ensuite utilisées uniquement dans la mesure où cela n'est pas incompatible avec la finalité du traitement. Ce principe de protection est garanti par l'article 36 de la loi DPA 2018. À l'instar de l'article 4, paragraphe 1, point b), de la directive (UE) 2016/680, cette disposition requiert que a) la finalité répressive pour laquelle les données à caractère personnel sont collectées à tout moment soit déterminée, explicite et légitime et que b) les données à caractère personnel ainsi collectées ne soient pas traitées d'une manière incompatible avec la finalité pour laquelle elles ont été collectées.

(44) Lorsque les autorités compétentes procèdent au traitement des données à des fins répressives, cela peut comprendre des finalités archivistiques, de recherche scientifique ou historique, et statistiques ([73]). Dans ces situations, la loi DPA 2018 précise également que l'archivage (ou le traitement à des finalités de recherche scientifique ou historique, et statistiques) n'est pas autorisé lorsqu'il est effectué dans le cadre de décisions prises à l'égard d'une personne concernée spécifique ou si cet archivage est susceptible de lui causer un préjudice ou une détresse ([74]).

2.4.3. *Exactitude et minimisation des données*

(45) Les données doivent être exactes et, si nécessaire, tenues à jour. Elles doivent également être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées. À l'instar de l'article 4, paragraphe 1, points c), d) et e), de la directive (UE) 2016/680, ces principes sont garantis par les articles 37 et 38 de la loi DPA 2018. Toutes les mesures raisonnables doivent être prises pour garantir que les données à caractère personnel qui sont inexactes ([75]) sont effacées ou

([71]) Guide relatif au traitement de données par les services répressifs, «Conditions pour le traitement de données sensibles» («Conditions for sensitive processing») (voir la note de bas de page n° 70).

([72]) Le traitement est effectué sans le consentement de la personne concernée lorsque: a) le consentement au traitement ne peut être donné par la personne concernée; b) on ne peut raisonnablement attendre du responsable du traitement qu'il obtienne le consentement de la personne concernée au traitement; c) le traitement doit être effectué sans le consentement de la personne concernée, étant donné que l'obtention du consentement de la personne concernée porterait atteinte à la protection visée au point 1) a).

([73]) Voir l'article 41, paragraphe 1, de la loi DPA 2018.

([74]) Voir l'article 41, paragraphe 2, de la loi DPA 2018.

([75]) L'article 205 de la loi DPA 2018 définit le terme «inexact» comme désignant des données à caractère personnel «incorrectes ou trompeuses». Les autorités du Royaume-Uni ont expliqué qu'il est fréquent que les données relatives à des enquêtes pénales soient incomplètes, mais qu'elles peuvent malgré tout être exactes.

rectifiées sans tarder ([76]), au regard des finalités répressives pour lesquelles elles sont traitées ([77]), et garantir que les données à caractère personnel qui sont inexactes, incomplètes ou ne sont plus à jour ne sont pas transmises ou mises à disposition pour l'une des fins répressives ([78]).

(46) Par ailleurs, de la même façon que l'article 7 de la directive (UE) 2016/680, le régime de protection des données du Royaume-Uni précise que les données à caractère personnel fondées sur des faits doivent être, dans la mesure du possible, distinguées de celles fondées sur des appréciations personnelles ([79]). Le cas échéant et autant que possible, une distinction claire doit être établie entre les données à caractère personnel de différentes catégories de personnes concernées, telles que les suspects, les personnes reconnues coupables d'une infraction pénale, les victimes d'une infraction pénale et les témoins ([80]).

2.4.4. *Limitation de la conservation*

(47) Conformément à l'article 5 de la directive (UE) 2016/680, les données ne doivent, en principe, pas être conservées plus longtemps que nécessaire pour atteindre les finalités pour lesquelles les données à caractère personnel sont traitées. En vertu de l'article 39 de la loi DPA 2018 et à l'instar de l'article 5 de ladite directive, il est interdit de conserver des données à caractère personnel pour l'une des fins répressives pendant une durée plus longue que nécessaire à la finalité pour laquelle ces données sont traitées. Le régime juridique du Royaume-Uni exige que des délais appropriés soient fixés pour la vérification régulière de la nécessité de conserver les données à caractère personnel à l'une des fins répressives. D'autres règles relatives aux pratiques en matière de conservation des données et les délais applicables ont été énoncés dans la législation pertinente et dans les orientations régissant les pouvoirs et le fonctionnement de la police. Par exemple, en Angleterre et au pays de Galles, le CBP relatif à la gestion des informations policières du collège des forces de police, ainsi que les orientations de la pratique professionnelle agréée pour la gestion des informations policières prévoient un cadre visant à garantir un processus cohérent de conservation, de vérification et de destruction fondé sur le risque pour la gestion des informations relatives aux fonctions policières opérationnelles ([81]). Ce cadre fixe des attentes claires pour tout le service en ce qui concerne la manière dont ces informations devraient être créées, partagées, utilisées et gérées au sein des différentes forces de police et d'autres agences et entre elles ([82]). On attend de la police qu'elle respecte le code de bonne pratique, et ce respect fait l'objet d'un examen par l'inspection de la police et des services d'incendie et de secours ([83]).

(48) Le service de police d'Irlande du Nord (PSNI) n'est pas tenu par la loi de suivre le CBP relatif à la gestion des informations policières. Toutefois, le cadre de la gestion des informations policières adopté en 2011 est complété par un manuel du service de police d'Irlande du Nord (PSNI Handbook) ([84]), qui établit des politiques et des procédures sur la manière dont le CBP relatif à la gestion des informations policières est appliqué en Irlande du Nord.

([76]) Article 38, paragraphe 1, point b), de la loi DPA 2018.

([77]) Selon le cadre explicatif du Royaume-Uni pour la discussion relative au niveau de protection adéquat, «cela permet de garantir que les droits des personnes concernées, aussi bien que les besoins opérationnels des autorités répressives, sont reconnus. Le point ci-dessus a été soigneusement étudié aux différentes étapes de l'élaboration du projet de loi sur la protection des données, puisqu'il peut exister des motifs opérationnels spécifiques et limités pour lesquels les données ne peuvent être rectifiées. Cela sera très probablement le cas si les données à caractère personnel inexactes concernées doivent être conservées sous leur forme originale à des fins probatoires» (voir le cadre explicatif du Royaume-Uni pour la discussion relative à l'adéquation, section F: Application des lois, page 21 (voir la note de bas de page n° 9).

([78]) Article 38, paragraphe 4, de la loi DPA 2018. En outre, au titre de l'article 38, paragraphe 5, de la loi DPA 2018, la qualité des données à caractère personnel doit être vérifiée avant leur transmission ou leur mise à disposition, les informations nécessaires qui permettent au destinataire d'évaluer le degré d'exactitude, d'exhaustivité et de fiabilité des données et leur niveau de mise à jour doivent être comprises dans toutes les transmissions de données à caractère personnel, et s'il s'avère, après leur transmission, que les données à caractère personnel sont incorrectes ou que la transmission était illicite, le destinataire doit en être informé sans délai.

([79]) Article 38, paragraphe 2, de la loi DPA 2018.

([80]) Article 38, paragraphe 3, de la loi DPA 2018.

([81]) Ce cadre garantit la cohérence de l'application de la conservation des données à caractère personnel acquises. La période d'examen dépend des infractions, qui se divisent en quatre groupes: 1) certaines questions relatives à la protection de la population; 2) autres infractions violentes et graves à caractère sexuel; 3) toutes les autres infractions; 4) divers. Pour plus de détails, voir les orientations de la pratique professionnelle agréée pour la gestion des informations policières (voir la note de bas de page n° 26).

([82]) D'après les informations communiquées par les autorités du Royaume-Uni, d'autres organisations sont libres de suivre les principes du CBP relatif à la gestion des informations policières si elles le souhaitent, par exemple, l'administration fiscale et douanière du Royaume-Uni et l'Agence nationale de lutte contre la criminalité adoptent volontairement de nombreux principes du CBP relatif à la gestion des informations policières pour assurer la cohérence de l'application des lois. En général, la plupart des organisations fourniront à leur personnel des politiques et des orientations spécifiques relatives à la manière de traiter les données à caractère personnel dans le cadre de leur mission et adaptées à leur organisation propre. D'habitude, cela comprend également une formation obligatoire.

([83]) Le CBP relatif à la gestion des informations policières a été publié en vertu des pouvoirs prévus par la loi de 1996 sur la police, qui permet au collège des forces de police de publier des codes de bonne pratique relatifs au fonctionnement efficace de la police. Tout code de bonne pratique élaboré au titre de cette loi doit être approuvé par le secrétaire d'État et fait l'objet d'une consultation avec l'Agence nationale de lutte contre la criminalité avant sa présentation au Parlement. L'article 39A, paragraphe 7, de la loi de 1996 sur la police exige que la police tienne dûment compte des codes publiés au titre de la loi de 1996 sur la police.

([84]) Manuel du service de police d'Irlande du Nord sur la gestion des informations policières, chapitre 1-6.

(49) En Écosse, les forces de police s'appuient sur les instructions permanentes relatives à la conservation des dossiers ([85]), sur lesquelles s'appuie la politique de gestion des dossiers du service de police d'Écosse ([86]). Les instructions permanentes fixent des règles de conservation spécifiques pour les dossiers conservés par la police écossaise.

(50) Outre l'exigence générale de vérifier les dossiers, qui s'applique à l'ensemble du Royaume-Uni, de plus amples détails sont énoncés dans les règles locales. À titre d'exemple, en ce qui concerne l'Angleterre et le pays de Galles, la loi sur la police et les preuves criminelles, telle que modifiée par la loi de 2012 sur la protection des libertés (Protection of Freedoms Act 2012 – la loi PoFA), prévoit la conservation d'empreintes digitales et des profils ADN ainsi qu'un régime spécifique pour les personnes non condamnées ([87]). La loi sur la protection des libertés a également créé le poste de commissaire responsable de la conservation et de l'utilisation du matériel biométrique (Commissioner for the Retention and Use of Biometric Material – «commissaire à la biométrie») ([88]). Des règles spécifiques concernant les photographies d'identité judiciaire sont énoncées dans le document 2017 Custody Image Review (Évaluation des photographies d'identité judiciaire 2017) ([89]). En ce qui concerne l'Écosse, la loi de 1995 sur les procédures pénales en Écosse prévoit les règles relatives à l'obtention et à la conservation des empreintes digitales et des échantillons biologiques ([90]). Comme pour l'Angleterre et le pays de Galles, la législation réglemente la conservation des données biométriques dans différents cas ([91]).

2.4.5. *Sécurité des données*

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

(52) Ces principes se reflètent à l'article 40 de la loi DPA 2018, selon lequel, à l'instar de l'article 4, paragraphe 1, point f), de la directive (UE) 2016/680, les données à caractère personnel traitées pour l'une des fins répressives doivent être traitées de façon à garantir une sécurité appropriée de ces données, à l'aide de mesures techniques ou organisationnelles appropriées. Cela inclut la protection contre le traitement non autorisé ou illicite des données et

([85]) Instructions permanentes relatives à la conservation des dossiers, disponibles à l'adresse suivante: https://www.scotland.police.uk/spa-media/nhobty5i/record-retention-sop.pdf.

([86]) Pour plus de détails sur la gestion des dossiers, voir les informations relatives aux Archives nationales d'Écosse (National Records of Scotland), disponibles à l'adresse suivante: https://www.nrscotland.gov.uk/record-keeping/records-management.

([87]) Les durées de conservation diffèrent selon qu'une personne a été condamnée ou non (articles 63I à 63KA de la loi PACE de 1984). Par exemple, dans le cas d'une personne adulte condamnée pour une infraction portant inscription dans les fichiers de police, ses empreintes digitales et son profil ADN peuvent être conservés indéfiniment (article 63I, paragraphe 2, de la loi PACE de 1984), alors que la conservation est limitée dans le temps lorsque la personne condamnée est âgée de moins de 18 ans, que l'infraction est une infraction «mineure» portant inscription dans les fichiers de police et que la personne n'a pas été condamnée auparavant (article 63K de la loi PACE de 1984). La durée de conservation dans le cas d'une personne arrêtée ou inculpée, mais non condamnée est limitée à trois ans (article 63F de la loi PACE de 1984). La prolongation de cette durée de conservation doit être approuvée par l'autorité judiciaire (article 63F, paragraphe 7, de la loi PACE de 1984). Dans le cas de personnes arrêtées ou inculpées pour des infractions mineures mais non condamnées, la conservation est impossible (articles 63D et 63H de la loi PACE de 1984).

([88]) L'article 20 de la loi PoFA de 2012 crée le poste de commissaire à la biométrie (Biometrics Commissioner). 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 pour la surveillance de la conservation et de l'utilisation de l'ADN et des empreintes digitales, ainsi que de la conservation pour des motifs de sécurité nationale, sous contrôle (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 (Governance Code for Public Appointments - GOV.UK, www.gov.uk) et son mandat prévoit qu'il ne peut être démis de ses fonctions par le ministère de l'intérieur que dans une série strictement définie de circonstances (incapacité d'accomplir ses fonctions pendant une période de trois mois, condamnation pour infraction pénale ou manquement aux obligations de son mandat, etc.)

([89]) Review of the Use and Retention of Custody Images (Évaluation de l'utilisation et de la conservation des photographies d'identité judiciaire), disponible à l'adresse suivante: https://www.gov.uk/government/publications/custody-images-review-of-their-use-and-retention.

([90]) Articles 18 et suivants de la loi de 1995 sur les procédures pénales en Écosse.

([91]) Les durées de conservation varient selon que la personne a été condamnée (article 18, paragraphe 3, de la loi de 1995 sur les procédures pénales en Écosse) ou qu'elle est mineure. Dans ce dernier cas, la durée de conservation est de trois ans à compter de la condamnation prononcée lors de l'audience des mineurs (children's hearing) (article 18E, paragraphe 8, de la loi de 1995 sur les procédures pénales en Écosse). Les données relatives aux personnes arrêtées mais non condamnées ne peuvent être conservées (article 18, paragraphe 3, de la loi de 1995 sur les procédures pénales en Écosse), à l'exception de certains cas spécifiques et selon la gravité de l'infraction (article 18A de la loi de 1995 sur les procédures pénales en Écosse). La loi de 2020 sur le commissaire écossais à la biométrie (Scottish Biometrics Commissioner Act 2020) (voir: https://www.legislation.gov.uk/asp/2020/8/contents) créé le poste de commissaire écossais à la biométrie, dont la mission est d'élaborer et de réviser les codes de bonne pratique (approuvés par le Parlement d'Écosse) relatifs à l'acquisition, la conservation, l'utilisation et la destruction des données biométriques à des fins de justice pénale et à des fins policières (article 7 de la loi de 2020 sur le commissaire écossais à la biométrie).

contre la perte, la destruction ou les dégâts d'origine accidentelle ([92]). L'article 66 de la loi DPA 2018 précise de plus que chaque responsable du traitement et chaque sous-traitant doivent mettre en œuvre des mesures techniques et organisationnelles pour garantir un niveau de sécurité adapté aux risques résultant du traitement des données à caractère personnel. D'après les notes explicatives, le responsable du traitement doit évaluer les risques et, sur la base de cette évaluation, prendre les mesures de sécurité adéquates, par exemple, le chiffrement ou des niveaux spécifiques d'habilitation de sécurité pour le personnel chargé de traiter les données ([93]). Ladite évaluation doit également tenir compte, par exemple, de la nature des données traitées ou de tous autres facteurs ou circonstances pertinents susceptibles d'avoir une incidence sur la sécurité du traitement.

(53) Le régime régissant le respect des principes de sécurité des données est très similaire à celui énoncé aux articles 29 à 31 de la directive (UE) 2016/680. En particulier, dans le cas d'une violation de données à caractère personnel touchant les données sous sa responsabilité, le responsable du traitement doit, conformément à l'article 67, paragraphe 1, de la loi DPA 2018, notifier cette violation au commissaire à l'information dans les meilleurs délais et, si possible, dans un délai de 72 heures au plus tard après en avoir pris connaissance ([94]). Cette obligation de notifier la violation de données à caractère personnel ne s'applique pas lorsque celle-ci n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes ([95]). Le responsable du traitement doit consigner les faits relatifs à toute violation de données à caractère personnel, ses effets et les mesures prises pour y remédier, de manière que le commissaire à l'information soit en mesure de vérifier le respect de la loi DPA ([96]). Si un sous-traitant prend connaissance d'une violation de sécurité, il doit en informer le responsable du traitement dans les meilleurs délais ([97]).

(54) En vertu de l'article 68, paragraphe 1, de la loi DPA 2018, lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et les libertés d'une personne, le responsable du traitement doit communiquer la violation à la personne concernée dans les meilleurs délais ([98]). La communication doit inclure les mêmes informations que la notification adressée au commissaire à l'information, qui sont décrites au considérant 53. Cette obligation ne s'applique pas si le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et si celles-ci ont été appliquées aux données à caractère personnel affectées par ladite violation. Elle ne s'applique également pas si le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et les libertés des personnes concernées n'est plus susceptible de se matérialiser. Enfin, le responsable du traitement n'est pas tenu de notifier la violation à la personne concernée si cela exige des efforts disproportionnés ([99]). Dans ce cas, les informations doivent être mises à la disposition de la personne concernée d'une autre manière tout aussi efficace, en procédant par exemple à une communication publique ([100]). Si le responsable du traitement n'a pas communiqué à la personne concernée la violation de données à caractère personnel la concernant, le commissaire à l'information, qui a été informé en vertu de l'article 67 de la loi DPA, peut, après avoir examiné si cette violation est susceptible d'engendrer un risque élevé, exiger du responsable du traitement qu'il procède à cette communication ([101]).

([92]) Conformément aux notes explicatives de la loi DPA 2018 (voir la note de bas de page n° 45), le responsable du traitement doit, en particulier: concevoir et organiser la sécurité en fonction de la nature des données à caractère personnel qu'il détient et du préjudice susceptible de résulter d'une violation de la sécurité; être transparent quant à la personne chargée, au sein de son organisation, de garantir la sécurité des informations; s'assurer qu'il dispose d'une sécurité physique et technique adéquate, soutenue par des politiques et des procédures solides et d'un personnel digne de confiance et bien formé; et être prêt à réagir promptement et efficacement à toute violation de la sécurité.

([93]) Point 221 des notes explicatives de la loi DPA 2018 (voir la note de bas de page n° 45).

([94]) En application de l'article 67, paragraphe 4, de la loi DPA 2018, la notification décrit la nature de la violation de données à caractère personnel (y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés), communique le nom et les coordonnées d'un point de contact, décrit les conséquences probables de la violation de données à caractère personnel, ainsi que les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel (y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives).

([95]) Article 67, paragraphe 2, de la loi DPA 2018.

([96]) Article 67, paragraphe 6, de la loi DPA 2018.

([97]) Article 67, paragraphe 9, de la loi DPA 2018.

([98]) En vertu de l'article 68, paragraphe 7, de la loi DPA 2018, le responsable du traitement peut limiter, en tout ou partie, la fourniture d'informations à la personne concernée dès lors et aussi longtemps que la restriction constitue, compte tenu des droits fondamentaux et des intérêts légitimes de la personne concernée, une mesure nécessaire et proportionnée pour a) éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires; b) éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes et aux poursuites en la matière ou à l'exécution de sanctions pénales; c) protéger la sécurité publique; d) protéger la sécurité nationale; e) protéger les droits et les libertés d'autrui.

([99]) Article 68, paragraphe 3, de la loi DPA 2018.

([100]) Article 68, paragraphe 5, de la loi DPA 2018.

([101]) Article 68, paragraphe 6, de la loi DPA 2018, sous réserve de la restriction prévue à l'article 68, paragraphe 8, de la loi DPA 2018.

2.4.6. *Transparence*

(55) Les personnes concernées doivent être informées des principales caractéristiques du traitement de leurs données à caractère personnel. Ce principe de protection des données se reflète à l'article 44 de la loi DPA 2018, qui, à l'instar de l'article 13 de la directive (UE) 2016/680, prévoit que le responsable du traitement a pour obligation générale de mettre à la disposition des personnes concernées les informations relatives au traitement de leurs données à caractère personnel (que ce soit en mettant les informations à la disposition du public de manière générale ou de toute autre façon) ([102]). Ces informations devant être mises à la disposition comprennent a) l'identité et les coordonnées du responsable du traitement; b) le cas échéant, les coordonnées du délégué à la protection des données; c) les finalités pour lesquelles le responsable du traitement procède au traitement de données à caractère personnel; d) l'existence du droit des personnes concernées de demander au responsable du traitement l'accès aux données à caractère personnel, leur rectification et leur effacement, ou la limitation de leur traitement; et e) l'existence du droit d'introduire une réclamation auprès du commissaire à l'information et les coordonnées dudit commissaire ([103]).

(56) Dans des cas particuliers, le responsable du traitement doit également fournir à la personne concernée – afin de lui permettre d'exercer ses droits en vertu de la loi DPA 2018 (par exemple, lorsque les données à caractère personnel traitées sont collectées à l'insu de la personne concernée) – des informations concernant a) la base juridique du traitement; b) les informations relatives à la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, aux critères utilisés pour déterminer cette durée; c) le cas échéant, les informations relatives aux catégories de destinataires des données à caractère personnel (y compris les destinataires dans les pays tiers ou au sein d'organisations internationales); d) toutes autres informations complémentaires nécessaires à l'exercice des droits de la personne concernée en vertu de la partie 3 de la loi DPA 2018 ([104]).

2.4.7. *Droits individuels*

(57) Plusieurs droits opposables doivent être conférés aux personnes concernées. Le chapitre 3 de la partie 3 de la loi DPA 2018 confère aux personnes des droits d'accès, de rectification, d'effacement et de limitation ([105]), qui sont comparables aux droits conférés en vertu du chapitre 3 de la directive (UE) 2016/680.

(58) Le droit d'accès est établi par l'article 45 de la loi DPA 2018. Premièrement, une personne est en droit d'obtenir, du responsable du traitement, la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées ([106]). Deuxièmement, lorsque les données à caractère personnel sont traitées, la personne concernée a le droit d'accéder à ces données et de recevoir les informations suivantes concernant le traitement: a) les finalités du traitement ainsi que ses bases juridiques; b) les catégories de données concernées; c) le destinataire auquel les données ont été communiquées; d) la durée pendant laquelle les données à caractère personnel sont conservées; e) l'existence du droit de la personne concernée à la rectification et à l'effacement des données à caractère personnel; f) le droit d'introduire une réclamation; et g) toute information relative à l'origine des données à caractère personnel concernées ([107]).

(59) En vertu de l'article 46 de la loi DPA 2018, la personne concernée a le droit d'exiger du responsable du traitement qu'il rectifie les données à caractère personnel inexactes qui la concernent. Le responsable du traitement doit rectifier (ou compléter, si les données sont inexactes parce qu'elles sont incomplètes) les données dans les meilleurs délais. Si les données à caractère personnel doivent être conservées à des fins probatoires, le responsable du traitement doit (au lieu de rectifier les données) limiter leur traitement ([108]).

([102]) Le guide relatif au traitement de données par les services répressifs fournit l'exemple suivant: «Vous disposez d'une déclaration générale de protection des données sur votre site web qui couvre les informations de base relatives à l'organisation, la finalité pour laquelle vous traitez des données à caractère personnel, les droits des personnes concernées et leur droit d'introduire une réclamation auprès du commissaire à l'information. Vous avez reçu des renseignements selon lesquels une personne était présente lorsque le crime a eu lieu. Lors de la première audition de cette personne, vous devez fournir les informations génériques, ainsi que les informations complémentaires afin de permettre l'exercice de ses droits. Vous pouvez limiter les informations relatives au traitement loyal que vous fournissez uniquement si ces informations nuiront à l'enquête que vous menez» [guide relatif au traitement de données par les services répressifs, «Quelles informations devrions-nous fournir à une personne?» («*What information should we supply to an individual*?»), disponible à l'adresse suivante: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib3].

([103]) Le guide relatif au traitement de données par les services répressifs indique que les informations fournies relatives au traitement de données à caractère personnel doivent être concises, compréhensibles et aisément accessibles; écrites dans un langage clair et simple, adaptées aux besoins des personnes vulnérables, telles que les enfants; et gratuites [guide relatif au traitement de données par les services répressifs, «Comment devrions-nous fournir cette information?» («*How should we provide this information?*»), disponible à l'adresse suivante: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib1].

([104]) Article 44, paragraphe 2, de la loi DPA 2018.

([105]) Pour une analyse détaillée des droits de la personne concernée, voir: Guide relatif au traitement de données par les services répressifs, «Droits individuels» («*Individual rights*»), disponible à l'adresse suivante: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/.

([106]) Article 45, paragraphe 1, de la loi DPA 2018.

([107]) Article 45, paragraphe 2, de la loi DPA 2018.

([108]) Article 46, paragraphe 4, de la loi DPA 2018.

(60) L'article 47 de la loi DPA 2018 confère aux personnes le droit à l'effacement et à la limitation du traitement. Le responsable du traitement doit ([109]) effacer dans les meilleurs délais les données à caractère personnel lorsque le traitement de ces données est susceptible d'enfreindre l'un des principes de protection des données, les motifs légaux du traitement, ou les garanties relatives à l'archivage et au traitement de données sensibles. Le responsable du traitement doit également effacer les données lorsqu'il y est légalement tenu. Si les données à caractère personnel doivent être conservées à des fins probatoires, le responsable du traitement doit (au lieu d'effacer les données) limiter leur traitement ([110]). Ledit responsable doit limiter le traitement de données à caractère personnel si une personne concernée conteste l'exactitude des données à caractère personnel, mais qu'il ne peut être déterminé si elles sont exactes ou non ([111]).

(61) Lorsqu'une personne concernée demande que les données à caractère personnel soient rectifiées ou effacées, ou que le traitement desdites données soit limité, le responsable du traitement doit lui indiquer par écrit si sa demande a été acceptée, et si elle a été refusée, informer la personne concernée des raisons du refus et des voies de recours possibles (le droit de la personne concernée d'introduire une demande auprès du commissaire à l'information pour vérifier que la limitation a bien été appliquée de manière licite, le droit d'introduire une réclamation auprès du commissaire à l'information, et le droit de demander une injonction judiciaire à se conformer aux dispositions légales) ([112]).

(62) Lorsque le responsable du traitement rectifie les données à caractère personnel reçues d'une autre autorité compétente, il doit en informer cette autorité ([113]). Lorsque le responsable du traitement rectifie, efface ou limite le traitement de données à caractère personnel qu'il a communiquées, ledit responsable doit en informer les destinataires, et les destinataires doivent également rectifier, effacer ou limiter le traitement des données à caractère personnel (dans la mesure où ils en conservent la responsabilité) ([114]).

(63) En outre, la personne concernée a le droit d'être informée dans les meilleurs délais, par le responsable du traitement, de toute violation de données à caractère personnel lorsque cette dernière est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes ([115]).

(64) En ce qui concerne tous ces droits de la personne concernée et à l'instar de ce qui est prévu à l'article 12 de la directive (UE) 2016/680, le responsable du traitement a pour obligation de veiller à ce que toute information fournie à la personne concernée le soit de façon concise, compréhensible et aisément accessible ([116]) et, si possible, sous la même forme que la demande ([117]). Le responsable du traitement doit donner suite à une demande de la personne concernée dans les meilleurs délais et, en principe et dans tous les cas, dans un délai d'un mois à compter de la demande ([118]). Lorsque le responsable du traitement a des doutes raisonnables quant à l'identité d'une personne, il peut demander que lui soient fournies des informations supplémentaires et retarder le traitement de la demande jusqu'à ce que l'identité de la personne concernée soit confirmée. Le responsable du traitement peut exiger le paiement de frais raisonnables ou refuser de donner suite à la demande lorsqu'il estime que cette dernière est manifestement infondée ([119]). L'ICO a fourni des orientations sur les cas dans lesquels une demande est considérée comme manifestement infondée ou excessive et dans lesquels le paiement de frais peut être exigé ([120]).

(65) En outre, en vertu de l'article 53, paragraphe 4, de la loi DPA 2018, le secrétaire d'État peut, par voie de règlements, préciser le montant maximum des frais.

([109]) Une personne concernée peut demander au responsable du traitement d'effacer les données à caractère personnel ou d'en limiter le traitement (mais les obligations du responsable d'effacer les données ou d'en limiter le traitement s'appliquent, qu'une telle demande soit faite ou non).

([110]) Article 46, paragraphe 4, et article 47, paragraphe 2, de la loi DPA 2018.

([111]) Article 47, paragraphe 3, de la loi DPA 2018.

([112]) Article 48, paragraphe 1, de la loi DPA 2018.

([113]) Article 48, paragraphe 7, de la loi DPA 2018.

([114]) Article 48, paragraphe 9, de la loi DPA 2018.

([115]) Article 68 de la loi DPA 2018.

([116]) Article 52, paragraphe 1, de la loi DPA 2018.

([117]) Article 52, paragraphe 3, de la loi DPA 2018.

([118]) L'article 54 de la loi DPA 2018 définit le «délai applicable» comme étant la période d'un mois, ou toute période plus longue pouvant être précisée dans les règlements, commençant en temps opportun (quand le responsable du traitement reçoit la demande en question; quand il reçoit les informations requises, le cas échéant, dans le cadre d'une demande en vertu de l'article 52, paragraphe 4 de la loi DPA; ou lorsque les frais exigés, le cas échéant, au titre de la demande en application de l'article 53 de la loi DPA sont versés).

([119]) Article 53, paragraphe 1, de la loi DPA 2018.

([120]) Selon les orientations de l'ICO, un responsable du traitement peut décider d'exiger le paiement de frais auprès de la personne concernée si la demande de cette dernière est manifestement infondée ou excessive, mais qu'il choisit tout de même d'y donner suite. Les frais doivent être raisonnables et pouvoir être justifiés. Guide relatif au traitement de données par les services répressifs «Demandes manifestement infondées et excessives» («*Manifestly unfounded and excessive requests*»), disponible à l'adresse suivante: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/manifestly-unfounded-and-excessive-requests/

2.4.7.1. Limitations des droits de la personne concernée et obligations en matière de transparence

(66) Une autorité compétente peut, dans certaines circonstances, limiter certains droits de la personne concernée, à savoir le droit d'accès ([121]), le droit à l'information ([122]), le droit d'être informé d'une violation de données à caractère personnel ([123]), et le droit d'être informé des raisons motivant le refus de donner suite à une demande de rectification et d'effacement ([124]). À l'instar du régime prévu au chapitre III de la directive (UE) 2016/680, l'autorité compétente ne peut appliquer la limitation que si, compte tenu des droits fondamentaux et des intérêts légitimes de la personne concernée, celle-ci constitue une mesure nécessaire et proportionnée pour: a) éviter de gêner une enquête, une recherche ou une procédure officielle ou judiciaire; b) éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes et aux poursuites en la matière ou à l'exécution de sanctions pénales; c) protéger la sécurité publique; d) protéger la sécurité nationale; e) protéger les droits et les libertés d'autrui.

(67) L'ICO a communiqué des orientations concernant l'application de ces limitations. Selon ces orientations, les responsables du traitement doivent effectuer une analyse au cas par cas pour concilier les droits de la personne avec le préjudice que causerait la divulgation. Ils doivent notamment justifier toute limitation appliquée comme étant nécessaire et proportionnée et ne peuvent appliquer que les limitations prévues si cela risque de nuire aux objectifs susmentionnés ([125]).

(68) Un certain nombre d'autres documents d'orientations ont été publiés par les autorités compétentes. Ils fournissent des informations détaillées concernant tous les aspects de la législation sur la protection des données, y compris l'application des limitations des droits des personnes concernées ([126]). À titre d'exemple, en ce qui concerne l'article 45, paragraphe 4, le manuel sur la protection des données du conseil du chef de la police nationale (Data Protection Manual of the National Police Chief's Counsel) dispose ce qui suit: «Il est essentiel de noter que les limitations ne peuvent être appliquées que dans la mesure où elles sont nécessaires et aussi longtemps que nécessaire. En conséquence, une application sans nuance de la limitation à toutes les données à caractère personnel d'un requérant ou l'application permanente de cette limitation ne sont pas autorisées. Sur ce dernier point, il est fréquent que les données à caractère personnel qui sont collectées à l'insu de la personne concernée, qui est suspectée dans le cadre d'une enquête, doivent être protégées dans un premier temps contre la divulgation à cette personne pour éviter de nuire à l'enquête lorsque cette dernière est en cours. À une date ultérieure cependant, la divulgation ne causerait aucun préjudice si les données à caractère personnel avaient été communiquées à la personne concernée lors de son audition. Les forces de police adoptent des processus qui garantissent que ces limitations ne sont appliquées que dans la mesure nécessaire et aussi longtemps que nécessaire» ([127]). Ces orientations donnent également des exemples des cas où chacune des limitations est susceptible d'être appliquée ([128]).

(69) De plus, en ce qui concerne la possibilité de limiter l'un des droits susmentionnés aux fins de la protection de la «sécurité nationale», un responsable du traitement peut déposer une demande de certificat signé par un ministre ou le procureur général (Attorney General) [ou l'avocat général pour l'Écosse (Advocate General for Scotland)] attestant qu'une limitation de ces droits est une mesure nécessaire et proportionnée pour protéger la sécurité nationale ([129]). Le gouvernement du Royaume-Uni a publié des orientations relatives aux certificats de sécurité nationale au titre de la loi DPA 2018, qui soulignent notamment que toute limitation des droits de la personne concernée pour la sauvegarde de la sécurité nationale doit être nécessaire et proportionnée ([130]) (pour plus de détails sur les certificats de sécurité nationale, voir les considérants 131 à 134).

([121]) Article 45, paragraphe 4, de la loi DPA 2018.
([122]) Article 44, paragraphe 4, de la loi DPA 2018.
([123]) Article 68, paragraphe 7, de la loi DPA 2018.
([124]) Article 48, paragraphe 3, de la loi DPA 2018.
([125]) Voir, par exemple, le Guide relatif au traitement de données par les services répressifs sur le droit d'accès, disponible à l'adresse suivante: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-of-access/#ib8.
([126]) Voir, par exemple, le manuel de protection des données à l'intention des professionnels de la protection des données des forces de police, publié par le conseil du chef de la police nationale (voir la note de bas de page n° 27) ou les orientations fournies par l'Office des fraudes graves, disponibles à l'adresse suivante: https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/data-protection/.
([127]) Manuel de protection des données du conseil du chef de la police nationale, page 140 (voir la note de bas de page n° 27).
([128]) Le manuel de protection des données du conseil du chef de la police nationale dispose que le fait d'«éviter de gêner une enquête, une recherche ou une procédure officielle ou judiciaire» est susceptible d'être pertinent pour les données à caractère personnel traitées dans le cadre d'enquêtes judiciaires médico-légales, de procédures juridictionnelles engagées en matière familiale, d'enquêtes disciplinaires internes non pénales, et d'enquêtes telles que l'enquête indépendante sur les abus sexuels commis contre des enfants (Independent Inquiry into Child Sexual Abuse); alors que le fait de «protéger les droits et libertés d'autrui» s'applique aux données à caractère personnel qui concerneraient également d'autres personnes ainsi que le requérant (manuel de protection des données du conseil du chef de la police nationale, page 140, voir la note de bas de page n° 27).
([129]) Article 79 de la loi DPA 2018.
([130]) Orientations du gouvernement du Royaume-Uni sur les certificats de sécurité nationale, 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.

(70) En outre, lorsqu'une limitation des droits de la personne concernée s'applique, l'autorité compétente doit informer cette dernière, dans les meilleurs délais, de ladite limitation, des raisons qui la motivent, et des voies de recours possibles, sauf si ces informations sont susceptibles de remettre en question les raisons motivant la limitation ([131]). Une garantie supplémentaire contre le recours abusif aux limitations est que le responsable du traitement doit consigner les raisons motivant la limitation des informations et mettre ce registre à la disposition du commissaire à l'information, si demande en est faite ([132]).

(71) Si le responsable du traitement refuse de fournir les informations de transparence supplémentaires, ou l'accès, ou qu'il refuse une demande de rectification, d'effacement ou de limitation du traitement, la personne peut demander au commissaire à l'information de vérifier que le responsable du traitement a bien appliqué la limitation de manière licite ([133]). La personne concernée peut également introduire une réclamation auprès du commissaire à l'information ou demander une injonction judiciaire ordonnant au responsable du traitement de donner suite à sa demande ([134]).

2.4.7.2. Prise de décision automatisée

(72) Les articles 49 et 50 de la loi DPA 2018 couvrent respectivement les droits relatifs à la prise de décision automatisée et les garanties à appliquer ([135]). À l'instar de ce que prévoit l'article 11 de la directive (UE) 2016/680, le responsable du traitement ne peut prendre une décision déterminante fondée exclusivement sur le traitement automatisé de données à caractère personnel que si elle est nécessaire ou autorisée par la loi ([136]). Une décision est déterminante si elle est susceptible de produire des effets juridiques défavorables pour la personne concernée ou d'affecter cette dernière de manière significative ([137]).

(73) Lorsque la loi oblige ou autorise le responsable du traitement à prendre une décision déterminante, l'article 50 de la loi DPA 2018 fixe les garanties qui s'appliqueront à cette décision (définie comme une «décision déterminante désignée»). Le responsable du traitement doit, dès que cela est raisonnablement réalisable, informer la personne concernée que cette décision a été prise. Dès lors, la personne concernée peut, dans un délai d'un mois, demander au responsable du traitement de revoir la décision ou d'en prendre une nouvelle qui n'est pas fondée exclusivement sur le traitement automatisé. Le responsable du traitement doit évaluer la demande et tenir la personne concernée informée de l'issue de cette évaluation. La loi DPA 2018 investit le secrétaire d'État du pouvoir d'adopter les règlements fixant des garanties supplémentaires ([138]). Aucun règlement de ce type n'a encore été adopté.

2.4.8. *Transferts ultérieurs*

(74) Le niveau de protection conféré aux données à caractère personnel qui sont transférées depuis une autorité répressive d'un État membre vers une autorité répressive 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 d'une autorité répressive 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.

([131]) Article 44, paragraphes 5 et 6, article 45, paragraphes 5 et 6, et article 48, paragraphe 4, de la loi DPA 2018.
([132]) Article 44, paragraphe 7, article 45, paragraphe 7, et article 48, paragraphe 6, de la loi DPA 2018.
([133]) Article 51 de la loi DPA 2018.
([134]) Article 167 de la loi DPA 2018.
([135]) En ce qui concerne le champ d'application du traitement automatisé, les notes explicatives de la loi DPA 2018 énoncent ce qui suit: «ces dispositions concernent la prise de décision entièrement automatisée et non le traitement automatisé. On parle de traitement automatisé (y compris de profilage) lorsqu'une opération effectuée sur les données ne requiert pas d'intervention humaine. Il y est régulièrement fait recours dans l'application des lois pour filtrer d'importants ensembles de données et obtenir des quantités pouvant être gérées par un opérateur humain. La prise de décision automatisée est une forme de traitement automatisé et exige que la décision finale soit prise sans influence humaine» (point 204 des notes explicatives de la loi DPA, voir la note de bas de page n° 45).
([136]) En plus des protections prévues dans la loi DPA, d'autres restrictions législatives dans le cadre juridique du Royaume-Uni s'appliquent aux autorités répressives et empêcheraient tout traitement automatisé (y compris le profilage) qui entraînerait une discrimination illégale. La loi de 1998 sur les droits de l'homme inscrit les droits énoncés dans la CEDH dans le droit du Royaume-Uni, et notamment le droit prévu à l'article 14 de la convention, qui interdit toute discrimination. De la même façon, la loi de 2010 sur l'égalité interdit toute discrimination contre des personnes présentant des caractéristiques protégées (en matière de sexe, de race, de handicap, etc.)
([137]) Article 49, paragraphe 2, de la loi DPA 2018.
([138]) Article 50, paragraphe 4, de la loi DPA 2018.

(75) Le régime des transferts internationaux du Royaume-Uni est régi par le chapitre 5 de la partie 3 de la loi DPA 2018 ([139]), et reflète l'approche adoptée au chapitre V de la directive (UE) 2016/680. En particulier, pour transférer des données à caractère personnel vers un pays tiers, une autorité compétente doit remplir trois conditions: a) le transfert doit être nécessaire à des fins répressives; b) le transfert doit être fondé sur: i) un règlement d'adéquation en ce qui concerne le pays tiers, ii) s'il ne repose pas sur un règlement d'adéquation, l'existence de garanties appropriées, ou iii) s'il ne repose pas sur une décision d'adéquation ou des garanties appropriées, il doit être fondé sur des circonstances particulières; et c) le destinataire du transfert doit être: i) une autorité pertinente (c'est-à-dire l'équivalent d'une autorité compétente) dans le pays tiers; ii) une «organisation internationale compétente», par exemple un organisme international qui exerce des fonctions correspondant à l'une des fins répressives; ou iii) une personne autre qu'une autorité pertinente, mais uniquement lorsque le transfert est strictement nécessaire à l'une des fins répressives; il n'existe pas de libertés ni de droits fondamentaux de la personne concernée qui prévalent sur l'intérêt public exigeant le transfert; un transfert des données à caractère personnel à une autorité pertinente du pays tiers serait inefficace ou inapproprié; et le destinataire est informé des fins pour lesquelles les données sont susceptibles d'être traitées ([140]).

(76) Les règlements d'adéquation relatifs à un pays tiers, un territoire, un secteur déterminé dans un pays tiers ou une organisation internationale, ou à une description ([141]) d'un tel pays, territoire, secteur ou d'une telle organisation sont adoptés par le secrétaire d'État. En ce qui concerne les normes à observer, le secrétaire d'État est tenu d'évaluer si ce territoire/secteur ou cette organisation assure un niveau de protection des données à caractère personnel adéquat. L'article 74A, paragraphe 4, de la loi DPA 2018 précise que, à cette fin, le secrétaire d'État doit prendre en considération un certain nombre d'éléments qui reflètent ceux énumérés à l'article 36 de la directive (UE) 2016/680 ([142]). À cet égard, depuis la fin de la période de transition, la partie 3 de la loi DPA 2018 constitue une législation nationale «dérivée de l'Union européenne» qui, comme il a été expliqué, sera interprétée par les juridictions du Royaume-Uni conformément à la jurisprudence de la Cour de justice pertinente datant d'avant la sortie du Royaume-Uni de l'Union et aux principes généraux du droit de l'Union, tels qu'ils étaient en vigueur juste avant la fin de la période de transition. Cela inclut la norme de niveau «essentiellement équivalent» qui s'appliquera donc aux évaluations d'adéquation effectuées par les autorités du Royaume-Uni.

(77) En ce qui concerne la procédure, les règlements sont soumis aux règles de procédure «générales» prévues par l'article 182 de la loi DPA 2018. Selon ladite procédure, le secrétaire d'État doit consulter le commissaire à l'information lorsqu'il propose d'adopter de futurs règlements d'adéquation au Royaume-

([139]) Ce nouveau cadre est devenu applicable à la fin de la période de transition, y compris le pouvoir du secrétaire d'État d'adopter des règlements d'adéquation. Cependant, les DPPEC (en particulier l'annexe 21, points 10 à 12, que les DPPEC insèrent à la loi DPA 2018) prévoient que certains transferts de données à caractère personnel pendant et après la période de transition soient traités comme s'ils reposaient sur des règlements d'adéquation. Ces transferts comprennent les transferts vers des pays tiers qui font l'objet d'une décision d'adéquation de l'Union européenne à la fin de la période de transition et vers des États membres de l'Union européenne, les États de l'AELE et le territoire de Gibraltar du fait de leur application de la directive en matière de protection des données dans le domaine répressif au traitement des données à des fins répressives [les États de l'AELE appliquent la directive (UE) 2016/680 en raison de leurs obligations au titre de l'acquis de Schengen]. Cela signifie qu'à la fin de la période de transition, les transferts vers ces pays peuvent se poursuivre de la même manière qu'avant la sortie de l'Union. À l'issue de la période de transition, le secrétaire d'État doit effectuer un examen des constats d'adéquation dans un délai de quatre ans.

([140]) Articles 73 et 77 de la loi DPA 2018.

([141]) Les autorités du Royaume-Uni ont expliqué que la description d'un pays ou d'une organisation internationale fait référence à une situation dans laquelle il serait nécessaire de procéder à une détermination spécifique ou partielle du caractère adéquat avec des limitations ciblées (par exemple, un règlement d'adéquation relatif à un type précis de transferts de données uniquement).

([142]) Voir l'article 74A, paragraphe 4, de la loi DPA 2018, qui prévoit que, pour évaluer le caractère adéquat du niveau de protection des données, «le secrétaire d'État doit, en particulier, tenir compte a) de l'état de droit, du respect des droits de l'homme et des libertés fondamentales, de la législation applicable, tant générale que sectorielle, y compris en ce qui concerne la sécurité publique, la défense, la sécurité nationale, le droit pénal et l'accès des autorités publiques aux données à caractère personnel, ainsi que de la mise en œuvre de cette législation, des règles en matière de protection des données, des règles professionnelles et des mesures de sécurité, y compris les règles régissant le transfert ultérieur de données à caractère personnel vers un autre pays tiers ou une autre organisation internationale, qui sont respectées dans ce pays ou par cette organisation internationale, de la jurisprudence, ainsi que des droits effectifs et opposables des personnes concernées et des possibilités de recours administratif et juridictionnel effectif pour les personnes concernées dont les données à caractère personnel sont transférées; b) de l'existence et du fonctionnement effectif d'une ou de plusieurs autorités de contrôle indépendantes qui sont chargées dans le pays tiers ou au sein de l'organisation internationale d'assurer et de faire respecter le régime juridique garantissant la protection des données, en disposant notamment des pouvoirs d'exécution adéquats, d'assister et de conseiller les personnes concernées dans l'exercice de leurs droits et dans leur coopération avec le commissaire; et c) des engagements internationaux pris par le pays tiers concerné ou par l'organisation internationale concernée, ou d'autres obligations découlant de conventions ou d'instruments juridiquement contraignants, ou encore découlant de leur participation à des systèmes multilatéraux ou régionaux, notamment en matière de protection des données à caractère personnel».

Uni ([143]). Une fois adoptés par le secrétaire d'État, lesdits règlements sont déposés devant le Parlement et soumis à la procédure «d'approbation tacite», en vertu de laquelle les deux Chambres du Parlement peuvent examiner les règlements et sont habilitées à voter une proposition d'annulation du règlement dans un délai de 40 jours ([144]).

(78) Conformément à l'article 74B, paragraphe 1, de la loi DPA 2018, les règlements d'adéquation doivent être réexaminés tous les quatre ans au minimum et le secrétaire d'État doit suivre, de manière permanente, les évolutions au sein des pays tiers et des organisations internationales susceptibles d'avoir une incidence sur les décisions d'adopter des règlements d'adéquation, ou de modifier ou d'abroger lesdits règlements. Lorsque le secrétaire d'État constate qu'un pays donné ou une organisation n'assure plus un niveau de protection des données à caractère personnel adéquat, il est tenu, dans la mesure nécessaire, de modifier ou d'abroger les règlements et d'engager des consultations avec le pays tiers ou l'organisation internationale concernés en vue de remédier à ce manquement.

(79) À l'instar de ce qui est prévu à l'article 37 de la directive (UE) 2016/680, en l'absence d'un règlement d'adéquation, un transfert de données à caractère personnel dans le contexte de l'application des lois serait possible si des garanties appropriées sont en place. Lesdites garanties sont assurées au moyen, soit a) d'un instrument juridiquement contraignant comprenant les garanties appropriées pour la protection des données à caractère personnel; soit b) d'une évaluation menée par le responsable du traitement qui, ayant évalué toutes les circonstances du transfert, estime qu'il existe des garanties appropriées au regard de la protection des données ([145]). Par ailleurs, lorsque les transferts sont fondés sur des garanties appropriées, la loi DPA 2018 prévoit que, outre la fonction de supervision normale de l'ICO, les autorités compétentes sont tenues de mettre à disposition des informations spécifiques relatives aux transferts vers l'ICO ([146]).

(80) Si un transfert ne repose pas sur une décision d'adéquation ou des garanties appropriées, il peut avoir lieu dans certaines circonstances spécifiques, dites «circonstances spéciales» ([147]). 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 pays tiers; d) dans des cas particuliers pour l'une des fins 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) ([148]). Il convient de noter que les points d) et e) ne s'appliquent pas si les droits et libertés de la personne concernée prévalent sur l'intérêt public du transfert ([149]). Cet ensemble de circonstances correspond aux situations et conditions spécifiques qualifiées de «dérogations» au titre de l'article 38 de la directive (UE) 2016/680.

(81) Dans ces circonstances, la date du transfert, l'heure, la justification, le nom du destinataire et toute autre information pertinente le concernant et la description des données à caractère personnel transférées doivent être documentés, et mis à la disposition du commissaire à l'information à sa demande ([150]).

(82) L'article 78 de la loi DPA 2018 régit le cas des «transferts ultérieurs», à savoir lorsque les données à caractère personnel qui ont été transférées du Royaume-Uni à un pays tiers sont ensuite transférées vers un autre pays tiers ou une organisation internationale. En vertu de l'article 78, paragraphe 1, le responsable du traitement du Royaume-Uni à l'origine du transfert doit imposer comme condition au transfert que les données ne soient pas ultérieurement transférées vers un pays tiers sans son autorisation. En outre, en vertu de l'article 78, paragraphe 3, et à l'instar de ce qui est prévu à l'article 35, paragraphe 1, point e), de la directive (UE) 2016/680, plusieurs exigences de fond

([143]) Voir le protocole d'accord entre le entre le secrétaire d'État au département du numérique, de la culture, des médias et du sport (Secretary of State for the Department for Digital, Culture, Media and Sport – DCMS) et le bureau du commissaire à l'information sur le rôle de l'ICO dans les nouvelles évaluations d'adéquation effectuées par le 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.

([144]) Au cours de ce délai de 40 jours, les deux Chambres du Parlement ont la possibilité, si elles le souhaitent, de voter contre les règlements; si ce vote est adopté, les règlements cesseront immédiatement d'avoir des effets juridiques.

([145]) Article 75 de la loi DPA 2018.

([146]) Selon l'article 75, paragraphe 3, de la loi DPA 2018, lorsqu'un transfert de données a lieu sur la base de garanties appropriées: a) ce transfert doit être documenté, b) la documentation est mise, sur demande, à la disposition du commissaire et c) la documentation doit inclure, notamment i) la date et l'heure du transfert, ii) le nom du destinataire et toute autre information pertinente le concernant, iii) la justification du transfert et iv) une description des données à caractère personnel transférées.

([147]) Guide relatif au traitement de données par les services répressifs, «Existe-t-il des circonstances spéciales?» («*Are there any special circumstances?*»), disponible à l'adresse suivante: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/international-transfers/#ib3).

([148]) Article 76 de la loi DPA 2018.

([149]) Article 76 de la loi DPA 2018.

([150]) Article 76, paragraphe 3, de la loi DPA 2018.

s'appliquent lorsqu'une telle autorisation est demandée. Plus spécifiquement, lorsque l'autorité compétente prend la décision d'autoriser ou non le transfert, elle doit s'assurer que le transfert ultérieur est nécessaire aux fins répressives et devrait tenir compte, entre autres, a) de la gravité des circonstances ayant conduit à la demande d'autorisation, b) des fins pour lesquelles les données à caractère personnel ont initialement été transférées, et c) des normes relatives à la protection des données à caractère personnel qui s'appliquent dans le pays tiers ou au sein de l'organisation internationale destinataire du transfert de données.

(83) En outre, lorsque la personne concernée par un transfert ultérieur depuis le Royaume-Uni avait initialement fait l'objet d'un transfert depuis l'Union européenne, des garanties supplémentaires s'appliquent.

(84) Premièrement, l'article 73, paragraphe 1, point b), de la loi DPA 2018 dispose, à l'instar de l'article 35, paragraphe 1, point c), de la directive (UE) 2016/680, que, dans le cas où les données à caractère personnel ont initialement été transmises au responsable du traitement ou à une autre autorité compétente ou mises de quelque autre manière à leur disposition par un État membre, ledit État membre, ou toute personne établie dans cet État membre qui constitue une autorité compétente aux fins de la directive (UE) 2016/680, doit avoir autorisé le transfert conformément au droit de l'État membre.

(85) Cependant, à l'instar de l'article 35, paragraphe 2, de la directive (UE) 2016/680, cette autorisation n'est pas requise lorsque a) le transfert est nécessaire aux fins de la prévention d'une menace grave et immédiate pour la sécurité publique d'un État membre ou d'un pays tiers ou pour les intérêts essentiels d'un État membre et que b) l'autorisation ne peut pas être obtenue en temps utile. Dans ce cas, l'autorité de l'État membre qui aurait été responsable de la décision d'autoriser ou non le transfert doit en être informée dans les meilleurs délais ([151]).

(86) Deuxièmement, la même approche s'applique en cas de données initialement transférées depuis l'Union européenne vers le Royaume-Uni, puis transférées ultérieurement par le Royaume-Uni vers un pays tiers qui les transférerait ensuite à un autre pays tiers. Dans ce cas, en vertu de l'article 78, paragraphe 4, l'autorité compétente du Royaume-Uni ne peut autoriser ce dernier transfert, en vertu de l'article 78, paragraphe 1, que si «l'État membre [qui a initialement transféré les données concernées], ou toute personne établie dans cet État membre qui constitue une autorité compétente aux fins de la directive en matière de protection des données dans le domaine répressif, a autorisé le transfert conformément au droit de l'État membre». Ces garanties sont importantes, car elles permettent aux autorités des États membres de garantir la continuité de la protection, conformément à la législation de l'Union européenne en matière de protection des données, tout au long de la «chaîne de transferts»

(87) Ce nouveau cadre relatif aux transferts internationaux est devenu applicable à la fin de la période de transition ([152]). Cependant, l'annexe 21, points 10 à 12 (introduits par les DPPEC), prévoit que certains transferts de données à caractère personnel, à partir de la fin de la période de transition, soient traités comme s'ils reposaient sur des règlements d'adéquation. Ces transferts comprennent les transferts vers un État membre, un État de l'AELE ou un pays tiers qui fait l'objet d'une décision d'adéquation de l'Union européenne à la fin de la période de transition, ainsi que vers le territoire de Gibraltar. En conséquence, les transferts vers ces pays peuvent se poursuivre de la même manière qu'avant la sortie du Royaume-Uni de l'Union. À l'issue de la période de transition, le secrétaire d'État doit effectuer un examen des constats d'adéquation dans un délai de quatre ans, c'est-à-dire avant 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.

2.4.9. *Responsabilité*

(88) Selon le principe de responsabilité, les autorités publiques 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.

(89) Ce principe se reflète à l'article 56 de la loi DPA 2018, qui introduit une obligation de responsabilité générale pour le responsable du traitement, c'est-à-dire l'obligation de mettre en œuvre les mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement de données à caractère personnel est effectué conformément aux exigences de la partie 3 de la loi DPA 2018. Ces mesures mises en œuvre doivent être réexaminées et actualisées, si nécessaire, et, lorsque cela est proportionné au regard des activités de traitement, comprendre les politiques appropriées en matière de protection des données.

([151]) Article 73, paragraphe 5, de la loi DPA 2018.

([152]) L'applicabilité de ce nouveau cadre doit être lue 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 du 31.12.2020, p. 14) («accord de commerce et de coopération UE-Royaume-Uni»), disponible à l'adresse suivante: https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:22020A1231(01)&from=FR.

(90) Conformément au chapitre IV de la directive (UE) 2016/680, les articles 55 à 71 de la loi DPA 2018 prévoient différents mécanismes pour garantir la responsabilité et permettre aux responsables du traitement et aux sous-traitants d'apporter la preuve qu'ils respectent leurs obligations. Plus particulièrement, les responsables du traitement sont tenus de mettre en œuvre des mesures de protection des données dès la conception et par défaut, c'est-à-dire de s'assurer que les principes de protection des données sont appliqués de façon effective, et sont tenus de tenir des registres pour toutes les catégories d'activités de traitement relevant de leur responsabilité (y compris les informations sur l'identité du responsable du traitement, les coordonnées du délégué à la protection des données, les finalités du traitement, les catégories des destinataires des divulgations, et une description des catégories de personnes concernées et de données à caractère personnel) et de maintenir ces registres à la disposition du commissaire à l'information, à sa demande. Le responsable du traitement et le sous-traitant doivent également tenir des journaux pour certaines opérations de traitement et les mettre à la disposition du commissaire à l'information ([153]). Les responsables du traitement sont également spécifiquement tenus de coopérer avec le commissaire à l'information dans l'exécution de leurs missions.

(91) La loi DPA 2018 énonce également des exigences supplémentaires lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes. Ces exigences comprennent une obligation d'effectuer des analyses d'impact relatives à la protection des données et de consulter le commissaire à l'information avant de procéder au traitement s'il ressort de cette analyse que le traitement engendrerait un risque élevé pour les droits et les libertés des personnes (en l'absence de mesures visant à atténuer ce risque).

(92) Le responsable du traitement doit par ailleurs désigner un délégué à la protection des données, sauf si ledit responsable est une juridiction ou une autre autorité judiciaire dans l'exercice de sa fonction juridictionnelle ([154]). Le responsable du traitement doit veiller à ce que le délégué à la protection des données soit associé à toutes les questions relatives à la protection des données à caractère personnel, qu'il dispose des ressources nécessaires ainsi que de l'accès aux données à caractère personnel et aux traitements et qu'il puisse exercer ses missions en toute indépendance. Les missions du délégué à la protection des données sont énoncées à l'article 71 de la loi DPA 2018, dont celles de fournir des informations et dispenser des conseils, de contrôler le respect des règles ainsi que de coopérer avec le commissaire à l'information et de faire office de point de contact pour ce dernier. Lorsqu'il accomplit ses tâches, le délégué à la protection des données doit tenir dûment compte des risques associés aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

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

2.5.1. *Surveillance indépendante*

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

(94) 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 ([155]). Le commissaire à l'information surveille également le traitement de données à caractère personnel par les autorités compétentes qui relèvent du champ d'application de la partie 3 de la loi DPA 2018 ([156]). Le commissaire à l'information est une «personne morale individuelle»: une entité juridique séparée constituée d'une seule personne. Le commissaire à l'information est soutenu dans son travail par un bureau. Le 31 mars 2020, le personnel permanent du Bureau du commissaire à l'information comptait 768 membres ([157]). Le ministère parrain du commissaire à l'information est le ministère du numérique, de la culture, des médias et du sport ([158]).

([153]) Article 62 de la loi DPA 2018.

([154]) Article 69 de la loi DPA 2018.

([155]) Article 36, paragraphe 2, point b), de la directive (UE) 2016/680.

([156]) Article 116 de la loi DPA 2018.

([157]) 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.

([158]) Un accord de gestion régit la relation entre les deux parties. Les principales responsabilités du DCMS, en tant que département parrain, sont notamment les suivantes: garantir que l'ICO bénéficie d'un financement et de ressources suffisants; représenter les intérêts de l'ICO auprès du Parlement et des autres départements du Gouvernement; garantir la mise en place d'un cadre national robuste de protection des données; et fournir des orientations et un soutien à l'ICO sur les questions organisationnelles, telles les questions immobilières, les baux et les 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).

(95) L'indépendance du commissaire est explicitement énoncée à l'article 52 du RGPD du Royaume-Uni, qui reflète les exigences fixées par l'article 52, paragraphes 1 à 3, du règlement (UE) 2016/679 du Parlement européen et du Conseil ([159]). Le commissaire doit exercer en toute indépendance ses missions et ses pouvoirs en vertu du RGPD du Royaume-Uni, demeurer libre de toute influence extérieure en ce qui concerne ces missions et ces pouvoirs, qu'elle soit directe ou indirecte, et ne doit ni solliciter ni accepter d'instructions de quiconque. Le commissaire doit en outre s'abstenir de tout acte incompatible avec ses fonctions et, pendant son mandat, n'exercer aucune activité professionnelle incompatible, rémunérée ou non.

(96) Les conditions pour la nomination et la révocation du commissaire à l'information sont énoncées à l'annexe 12 de la loi DPA 2018. Le commissaire à l'information est nommé par la Reine suivant les recommandations du Gouvernement, en vertu d'une compétition juste et ouverte. Le candidat doit posséder les qualifications, les aptitudes et les compétences adéquates. Conformément au code de gouvernance pour les nominations publiques, un panel d'évaluation consultatif dresse une liste des candidats retenus ([160]). Avant que le secrétaire d'État au département du numérique, de la culture, des médias et du sport n'arrête sa décision, le comité spécial compétent du Parlement est tenu d'effectuer un examen préalable à la nomination. L'avis de la commission est ensuite rendu public ([161]).

(97) Le commissaire à l'information est nommé pour une durée maximale de sept ans. Le commissaire à l'information peut être démis de ses fonctions par la Reine à la suite d'une requête émise par les deux Chambres ([162]). Aucune demande de révocation du commissaire à l'information ne peut être présentée à l'une ou l'autre des Chambres du Parlement, sauf si un ministre dépose un rapport à la Chambre concernée exposant qu'il est convaincu que le commissaire à l'information a commis une faute grave et/ou que le commissaire ne remplit plus les conditions nécessaires à l'exercice de ses fonctions ([163]).

(98) Le financement du commissaire à l'information provient de trois sources: i) les frais de protection de données payés par les responsables du traitement qui sont fixés par les règlements du secrétaire d'État ([164]) et constituent 85 à 90 % du budget annuel du bureau ([165]); ii) les subventions susceptibles d'être versées par le gouvernement au commissaire à l'information et servant principalement à payer les coûts d'exploitation du commissaire à l'information en ce qui concerne les missions qui ne sont pas liées à la protection des données ([166]); et iii) les frais facturés pour la prestation de services ([167]). À l'heure actuelle, aucun frais de cette sorte n'est facturé.

(99) Les fonctions générales du commissaire à l'information en ce qui concerne le traitement de données à caractère personnel qui relève du champ d'application de la partie 3 de la loi DPA 2018 sont énoncées à l'annexe 13 de la loi DPA 2018. Les missions comprennent la surveillance et le contrôle de l'application de la partie 3 de la loi DPA 2018, la sensibilisation du public, la dispense de conseils au Parlement, au gouvernement et à d'autres institutions au sujet des mesures législatives et administratives, la sensibilisation des responsables du traitement et des sous-traitants aux obligations qui leur incombent, la fourniture d'informations à une personne concernée sur l'exercice de

([159]) 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) (JO L 119 du 4.5.2016, p. 1).

([160]) Code de gouvernance pour les nominations publiques, disponible à l'adresse suivante: https://www.gov.uk/government/publications/governance-code-for-public-appointments.

([161]) 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.

([162]) Une «requête» («*adress*») est une proposition déposée devant le Parlement dans le but d'informer le monarque des opinions du Parlement sur une question en particulier.

([163]) Annexe 12, point 3, de la loi DPA 2018.

([164]) Article 137 de la loi DPA 2018.

([165]) 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, de la loi DPA 2018, dresse une liste des éléments que le secrétaire d'État doit prendre en considération lorsqu'il adopte des règlements précisant les montants dont diverses organisations doivent s'acquitter. L'article 138, paragraphe 1, et l'article 182 de la loi DPA 2018 comprennent en outre une prescription légale exigeant du secrétaire d'État qu'il consulte le commissaire à l'information et d'autres représentants de personnes susceptibles d'être concernées par les règlements, avant que ces derniers ne soient adoptés, de manière que leurs avis puissent être pris en considération. Par ailleurs, conformément à l'article 138, paragraphe 2, de la loi DPA 2018, le commissaire à l'information est tenu de maintenir les règlements relatifs aux frais à l'étude et peut soumettre des propositions de modifications desdits règlements au secrétaire d'État. Enfin, les règlements sont soumis à une procédure de ratification et ne peuvent être adoptés sans avoir été approuvés au préalable par chaque Chambre du Parlement par voie de résolution, sauf lorsque lesdits règlements sont simplement destinés à tenir compte d'une augmentation de l'indice des prix de détail (auquel cas ils seront soumis à une procédure d'approbation tacite).

([166]) 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 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 n° 158).

([167]) Article 134 de la loi DPA 2018.

ses droits et la conduite d'enquêtes. Afin de préserver l'indépendance du pouvoir judiciaire, le commissaire à l'information n'est pas habilité à exercer ses fonctions relatives au traitement de données à caractère personnel par une personne dans l'exercice de sa fonction juridictionnelle, ou par une juridiction ou un tribunal dans l'exercice de leur fonction juridictionnelle. Néanmoins, la surveillance du pouvoir judiciaire est assurée par des organismes spécialisés, dont il est question ci-après.

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

(100) Le commissaire dispose de compétences générales d'enquête, de rectification, d'autorisation et de consultation en ce qui concerne le traitement de données à caractère personnel auquel s'applique la partie 3 de la loi DPA 2018. Le commissaire dispose de compétences pour notifier au responsable du traitement ou au sous-traitant une violation alléguée de la partie 3, avertir un responsable du traitement ou un sous-traitant du fait que les opérations de traitement envisagées sont susceptibles de violer les dispositions de la partie 3 et rappeler à l'ordre un responsable du traitement ou un sous-traitant lorsque les opérations de traitement ont entraîné une violation des dispositions de la partie 3. En outre, de sa propre initiative ou sur demande, le commissaire peut émettre des avis à l'attention du parlement britannique, du gouvernement ou d'autres institutions et organismes ainsi que du public, sur toute question relative à la protection des données à caractère personnel ([168]).

(101) En outre, le commissaire dispose de compétences pour:

— ordonner au responsable du traitement et au sous-traitant (et, dans certaines circonstances, à toute autre personne) de fournir les informations nécessaires en remettant un avis d'information («avis d'information») ([169]),

— mener des enquêtes et des audits en émettant un avis d'évaluation, aux fins desquels le responsable du traitement ou le sous-traitant est susceptible de devoir permettre au commissaire d'accéder aux locaux déterminés, d'inspecter ou d'étudier les documents ou l'équipement, d'interroger des personnes traitant les données à caractère personnel pour le compte du responsable du traitement («avis d'évaluation») ([170]),

— obtenir autrement l'accès aux documents du responsable du traitement ou du sous-traitant et aux locaux de ces derniers, en application de l'article 154 de la loi DPA 2018 («pouvoirs d'accès et d'inspection»),

— adopter des mesures correctrices, y compris par voie d'avertissements et de rappels à l'ordre, ou donner des ordres au moyen d'un avis d'exécution, qui oblige le responsable du traitement ou le sous-traitant à prendre ou à s'abstenir de prendre des mesures déterminées («avis d'exécution») ([171]), et

— infliger des amendes administratives sous la forme d'un avis de sanction («avis de sanction») ([172]).

(102) La politique d'intervention réglementaire (Regulatory Action Policy) de l'ICO définit les circonstances dans lesquelles le commissaire émettra respectivement un avis d'information, d'évaluation, d'exécution et de sanction ([173]). Un avis d'exécution peut imposer des exigences que le commissaire estime appropriées pour remédier au manquement. Un avis de sanction exige de la personne qu'elle verse au commissaire à l'information un montant précisé dans l'avis. Un avis de sanction peut être émis lorsqu'un non-respect de certaines des dispositions de la loi DPA 2018 ([174]) a été constaté ou peut être remis à un responsable du traitement ou à un sous-traitant qui n'a pas respecté un avis d'information, d'évaluation ou d'exécution.

(103) Plus particulièrement, lorsqu'il décide s'il convient d'adresser un avis de sanction à un responsable du traitement ou à un sous-traitant et qu'il détermine le montant de la sanction, le commissaire à l'information doit prendre en considération les éléments énumérés à l'article 155, paragraphe 3, de la loi DPA 2018, dont la nature et la gravité du manquement, le fait que le manquement a été commis 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

([168]) Annexe 13, point 2, de la loi DPA 2018.
([169]) Article 142 de la loi DPA 2018 (sous réserve des limitations de l'article 143 de la loi DPA 2018).
([170]) Article 146 de la loi DPA 2018 (sous réserve des limitations de l'article 147 de la loi DPA 2018).
([171]) Articles 149 à 151 de la loi DPA 2018 (sous réserve des limitations de l'article 152 de la loi DPA 2018).
([172]) Article 155 de la loi DPA 2018 (sous réserve des limitations de l'article 156 de la loi DPA 2018).
([173]) Politique d'action réglementaire, disponible à l'adresse suivante: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.
([174]) L'ICO peut notamment émettre un avis de sanction dans le cas d'un non-respect visé à l'article 149, paragraphe 2, 3, 4 ou 5, de la loi DPA 2018.

de responsabilité du responsable du traitement ou du sous-traitant (compte tenu des mesures techniques et organisationnelles qu'ils ont mises en œuvre), tout manquement pertinent commis précédemment par le responsable du traitement ou le sous-traitant; les catégories de données à caractère personnel concernées par le manquement et la question de savoir si la sanction serait effective, proportionnée et dissuasive.

(104) Le montant maximal de la sanction qui peut être imposée par voie d'avis de sanction est de a) 17 500 000 livres sterling (GBP) pour un non-respect des principes de protection des données (articles 35, article 36, article 37, article 38, paragraphe 1, article 39, paragraphe 1, et article 40 de la loi DPA 2018), des obligations en matière de transparence et des droits individuels (articles 44, 45, 46, 47, 48, 49, 52 et 53 de la loi DPA 2018), et des principes relatifs aux transferts internationaux de données à caractère personnel (articles 73, 75, 76, 77 ou 78 de la loi DPA 2018); et de b) 8 700 000 GBP pour tout autre manquement ([175]). Concernant le non-respect d'un avis d'information, d'évaluation ou d'exécution le montant maximal de la sanction qui peut être imposée par voie d'avis de sanction est de 17 500 000 GBP.

(105) D'après ses derniers rapports annuels (2018-2019 ([176]), 2019-2020 ([177])), le commissaire à l'information a mené plusieurs enquêtes relatives au traitement de données à caractère personnel par les autorités répressives. Par exemple, le commissaire a conduit une enquête et publié un avis en octobre 2019 concernant le recours à la technologie de reconnaissance faciale dans les lieux publics à des fins répressives. L'enquête s'est particulièrement concentrée sur l'usage des capacités de reconnaissance faciale en temps réel par la police du pays de Galles du Sud et le service de police métropolitaine (Metropolitan Police Service – MPS). En outre, le commissaire a mené une enquête sur la base de données «Gang matrix» (matrice des gangs) du MPS ([178]), et a constaté une série de graves violations de la législation sur la protection des données susceptibles d'ébranler la confiance du public en la matrice et l'utilisation des données.

(106) En novembre 2018, le commissaire à l'information a émis un avis d'exécution à la suite duquel le MPS a pris les mesures nécessaires pour renforcer la sécurité et la responsabilité et garantir que les données soient utilisées de manière proportionnée.

(107) Un autre exemple d'une récente mesure répressive est l'amende de 325 000 GBP infligée en mai 2018 par le commissaire à l'encontre du ministère public, après la perte de plusieurs DVD non cryptés contenant des enregistrements d'interrogatoires de police. Par ailleurs, le commissaire à l'information a conduit des enquêtes sur des questions plus générales, par exemple, au cours du premier semestre de l'année 2020, sur l'utilisation de l'extraction des téléphones portables à des fins policières et le traitement des données à caractère personnel des victimes.

(108) Outre ces pouvoirs d'application des règles du commissaire à l'information, certaines violations de la législation sur la protection des données constituent des infractions et peuvent, à ce titre, faire l'objet de sanctions pénales (article 196 de la loi DPA 2018). Cela vaut, par exemple, pour l'obtention et la divulgation de données à caractère personnel sans le consentement du responsable du traitement et la divulgation de données à caractère personnel à une personne tierce sans le consentement du responsable du traitement ([179]); la nouvelle identification d'informations qui sont des données à caractère personnel anonymisées sans le consentement du responsable du traitement en charge de l'anonymisation de données à caractère personnel ([180]); l'obstruction intentionnelle du commissaire dans l'exercice de ses pouvoirs en ce qui concerne l'inspection des données à caractère personnel, conformément aux obligations internationales ([181]), les fausses déclarations en réponse à un avis d'information, ou la destruction d'informations en rapport avec les avis d'information et d'évaluation ([182]).

(109) Le commissaire à l'information est également tenu, au titre de l'article 139 de la loi DPA 2018, de déposer devant chaque Chambre du Parlement un rapport général portant sur l'exercice de ses fonctions en vertu de cette loi ([183]).

([175]) Article 157 de la loi DPA 2018.

([176]) Rapport annuel et 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.

([177]) Rapport annuel 2019-2020 du commissaire à l'information (voir la note de bas de page n° 157).

([178]) Une base de données recensant les renseignements relatifs aux membres de gang présumés et aux victimes de crimes liés aux gangs.

([179]) Article 170 de la loi DPA 2018.

([180]) Article 171 de la loi DPA 2018.

([181]) Article 119 de la loi DPA 2018.

([182]) Articles 144 et 148 de la loi DPA 2018.

([183]) Comme énoncé dans l'accord de gestion, le rapport annuel doit: i) couvrir toute entreprise, filiale ou coentreprise sous le contrôle de l'ICO; ii) être conforme au manuel d'information financière du Trésor (Treasury's Financial Reporting Manual – FReM); iii) contenir une déclaration de gouvernance, énonçant les manières dont le comptable a géré et contrôlé les ressources utilisées au sein de l'organisation au cours de l'année, démontrant l'adéquation de la gestion des risques par l'organisation pour la réalisation de ses buts et objectifs; et iv) exposer les activités et performances principales au cours de l'exercice financier précédent et présenter sous forme résumée la planification prévisionnelle (accord de gestion 2018-2021, point 3.26, voir la note de bas de page n° 158).

2.5.2. *Surveillance du pouvoir judiciaire*

(110) La surveillance du traitement de données à caractère personnel par les juridictions et le pouvoir judiciaire est double. Lorsqu'un titulaire d'une fonction juridictionnelle ou une juridiction n'agit pas dans l'exercice de sa fonction juridictionnelle, la surveillance est assurée par le commissaire à l'information. Lorsque le responsable du traitement agit dans l'exercice de sa fonction juridictionnelle, l'ICO ne peut exercer ses fonctions de surveillance ([184]) et la surveillance est assurée par des organismes spéciaux. Cela reflète l'approche adoptée par l'article 32 de la directive (UE) 2016/680.

(111) 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 ([185]). En outre, le président de la Haute Cour et le Premier président des tribunaux ont publié une déclaration de protection des données ([186]) 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 ([187]) et d'Écosse ([188]).

(112) 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 ([189]). 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 ([190]).

(113) En Écosse, le Lord président (le doyen des juges) a nommé un juge délégué à la surveillance des données pour enquêter sur toute réclamation reposant sur des motifs de 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 ([191]).

(114) Enfin, au sein de la Cour suprême, l'un des juges est désigné pour surveiller la protection des données.

([184]) Article 117 de la loi DPA 2018.

([185]) Le panel est chargé de fournir des orientations et de dispenser des formations aux juges. Il traite également les réclamations des personnes concernées en ce qui concerne le traitement de données à caractère personnel par les juridictions, les tribunaux et les personnes dans l'exercice de leur fonction juridictionnelle. Le tribunal spécialisé œuvre à fournir les moyens grâce auxquels toute réclamation peut être résolue. Si l'auteur d'une réclamation était insatisfait d'une décision du tribunal spécialisé, et s'il a apporté des éléments de preuve supplémentaires, ledit tribunal pourrait réexaminer sa décision. Alors que le tribunal spécialisé lui-même n'impose aucune sanction financière, s'il estime qu'il y a violation suffisamment grave de la loi DPA 2018, il peut transmettre la réclamation au Bureau d'enquête sur la conduite judiciaire (Judicial Conduct Investigation Office – JCIO), qui l'examinera. Si la réclamation est acceptée, il incombe au Lord chancelier (Lord Chancellor) et au président de la Haute Cour (Lord Chief Justice) (ou tout juge de haut rang appelé à agir en son nom) de décider des mesures à prendre à l'encontre du titulaire de la fonction. Cela peut comprendre, par ordre de gravité: la dispense de conseils formels, l'émission d'avertissements et de rappels à l'ordre formels, et, finalement, la destitution de la fonction. Si une personne n'est pas satisfaite de la manière dont sa réclamation a été examinée par le JCIO, il lui est possible de déposer une plainte auprès du médiateur pour les nominations et la conduite judiciaires (Judicial Appointments and Conduct Ombudsman) (voir: https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman). Le médiateur est habilité à demander au JCIO de réexaminer la réclamation et à proposer que l'auteur de la réclamation soit indemnisé s'il estime que celui-ci a subi un préjudice résultant d'une mauvaise administration.

([186]) 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

([187]) 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.

([188]) 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

([189]) 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.

([190]) 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. Une telle réclamation pourrait finalement donner lieu à: aucune mesure ultérieure, des conseils, une formation ou un mentorat, un avertissement informel ou formel, un avertissement final, la limitation de la pratique ou la saisine d'un tribunal prévu par la loi. Le code de bonne pratique relatif aux réclamations du 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.

([191]) 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).

2.5.3. *Voies de recours*

(115) 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 de réparation du préjudice subi.

(116) Premièrement, une personne concernée a le droit de déposer une réclamation auprès du commissaire à l'information si elle estime que, en ce qui concerne les données à caractère personnel la concernant, une violation de la partie 3 de la loi DPA 2018 a eu lieu ([192]). Comme décrit aux considérants 100 et 109, le commissaire à l'information est habilité à évaluer le respect de la loi DPA 2018 par le responsable du traitement et le sous-traitant, d'exiger du responsable du traitement et du sous-traitant qu'ils prennent les mesures nécessaires en cas de non-respect et d'infliger des amendes.

(117) Deuxièmement, la loi DPA 2018 prévoit un droit de recours contre le commissaire à l'information. Si le commissaire échoue à «faire avancer» ([193]) une réclamation introduite par la personne concernée, l'auteur de la réclamation dispose d'un recours juridictionnel, car il peut demander au tribunal de première instance ([194]) d'ordonner au commissaire de prendre les mesures adéquates pour donner suite à la réclamation ou pour informer l'auteur de la réclamation de l'avancement de la réclamation ([195]). En outre, toute personne qui reçoit l'un des avis susmentionnés (avis d'information, d'évaluation, d'exécution ou de sanction) de la part du commissaire peut former un recours devant un tribunal de première instance. Si le tribunal estime que la décision du commissaire n'est pas conforme à la loi ou que le commissaire à l'information aurait dû exercer son pouvoir discrétionnaire d'une manière différente, le tribunal doit faire droit au recours, ou substituer à la décision du commissaire un autre avis ou une autre décision que le commissaire à l'information aurait pu émettre ou prendre ([196]).

(118) Troisièmement, les personnes peuvent introduire un recours juridictionnel à l'encontre des responsables du traitement et des sous-traitants directement devant les juridictions en vertu de l'article 167 de la loi DPA 2018. Si, à la suite d'une demande de la personne concernée, une juridiction est convaincue qu'il y a eu violation des droits de la personne concernée au titre de la législation sur la protection des données, elle peut ordonner au responsable du traitement, ou à un sous-traitant agissant au nom dudit responsable, de prendre les mesures définies dans l'injonction ou de s'en abstenir. Par ailleurs, en vertu de l'article 169 de la loi DPA 2018, toute personne qui subit un préjudice en raison d'une violation d'une exigence prévue par la législation sur la protection des données (dont par la partie 3 de la loi DPA 2018) autre que le RGPD du Royaume-Uni, peut obtenir, de la part du responsable du traitement ou du sous-traitant, une indemnisation pour le préjudice subi, sauf si ledit responsable ou sous-traitant prouve qu'il n'est en aucune manière responsable du fait générateur du préjudice. Le préjudice comprend aussi bien la perte financière que le préjudice n'entraînant aucune perte financière, tel que la détresse.

(119) Quatrièmement, dès lors qu'une personne estime que ses droits, y compris ses droits au respect de la vie privée et à la protection des données, ont été violés par les autorités publiques, elle peut obtenir réparation devant les juridictions du Royaume-Uni en application de la loi de 1998 sur les droits de l'homme. Les responsables du traitement au titre de la partie 3 de la loi DPA 2018, c'est-à-dire les autorités compétentes, sont toujours des autorités publiques au sens de la loi de 1998 sur les droits de l'homme. Toute personne qui prétend que l'autorité publique a agi (ou propose d'agir) d'une manière incompatible avec un droit garanti par la CEDH et, partant, illicite en vertu de l'article 6, paragraphe 1, de la loi de 1998 sur les droits de l'homme, peut engager une procédure à l'encontre de l'autorité devant la juridiction ou le tribunal approprié, ou invoquer les droits concernés dans toute procédure juridictionnelle, si elle est (ou serait) victime de l'acte illicite ([197]).

([192]) Article 165 de la loi DPA 2018.

([193]) L'article 166 de la loi DPA 2018 fait spécifiquement référence aux situations suivantes: a) le commissaire ne prend pas les mesures appropriées pour donner suite à la réclamation, b) le commissaire ne fournit pas à l'auteur de la réclamation les informations relatives à l'état d'avancement de la réclamation, ou à l'issue de celle-ci, avant la fin du délai de trois mois à compter de la réception de la réclamation par le commissaire ou c) si son examen de la réclamation n'est pas mené à terme au cours de ce délai, le commissaire ne fournit pas ces informations à l'auteur de la réclamation dans un délai supplémentaire de trois mois.

([194]) Le tribunal de première instance est la juridiction compétente pour examiner les recours formés à l'encontre de décisions prises par les organismes réglementaires du gouvernement. Dans le cas d'une décision prise par le commissaire à l'information, la chambre compétente est la division de la réglementation générale (General Regulatory Chamber), qui est compétente pour l'ensemble du Royaume-Uni.

([195]) Article 166 de la loi DPA 2018.

([196]) Articles 161 et 162 de la loi DPA 2018.

([197]) Voir l'affaire Brown/Commissioner of the Met de 2016, dans laquelle la juridiction a accordé réparation à la plaignante dans le contexte de la protection des données dans le cadre d'une action intentée contre la police. La juridiction a statué en faveur de la plaignante, faisant droit à ses allégations de violation des obligations découlant de la loi DPA 1998, de violation de la loi de 1998 sur les droits de l'homme (et des droits liés prévus à l'article 8 de la CEDH) et d'usage abusif de données relatives à la vie privée (la partie défenderesse a finalement admis qu'elle enfreignait la loi DPA et la CEDH, de sorte que le jugement se concentrait sur la mesure corrective adéquate). En raison de ces violations, la juridiction a accordé une indemnisation pécuniaire à la plaignante.

(120) 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 ([198]). La juridiction peut en outre déclarer qu'une disposition du droit primaire est incompatible avec un droit garanti au titre de la CEDH.

(121) Enfin, après avoir épuisé toutes les voies de recours nationales, une personne peut obtenir réparation devant la Cour européenne des droits de l'homme pour violation des droits garantis par la CEDH.

2.6. **Partage ultérieur**

(122) Le droit du Royaume-Uni autorise, sous certaines conditions, le partage de données par une autorité répressive avec d'autres autorités britanniques pour des finalités autres que celles pour lesquelles lesdites données ont initialement été collectées (dit «partage ultérieur»).

(123) De manière similaire à ce qui est prévu à l'article 4, paragraphe 2, de la directive (UE) 2016/680, l'article 36, paragraphe 3, de la loi DPA 2018 autorise que les données à caractère personnel collectées par une autorité compétente à une fin répressive puissent être traitées ultérieurement (que ce soit par le même responsable du traitement ou un autre) pour toute autre fin répressive, à la condition que le responsable du traitement soit autorisé par la loi à traiter les données à cette autre fin et que le traitement soit nécessaire et proportionné ([199]). Dans cette situation, toutes les garanties prévues par la partie 3 de la loi DPA 2018 et analysées ci-dessus s'appliquent au traitement effectué par l'autorité destinataire.

(124) Dans l'ordre juridique du Royaume-Uni, différentes lois autorisent explicitement le partage ultérieur. En particulier, i) la loi de 2017 sur l'économie numérique (Digital Economy Act 2017) permet le partage entre les autorités publiques à plusieurs fins, par exemple en cas de fraude commise à l'encontre du secteur public qui entraînerait une perte ou un risque de perte pour une autorité publique ([200]) ou en cas de dette due à une autorité publique ou à la Couronne ([201]); ii) la loi de 2013 sur la criminalité et les tribunaux autorise le partage d'informations avec l'Agence nationale de lutte contre la criminalité ([202]) pour la lutte, les enquêtes et les poursuites contre la grande criminalité et la criminalité organisée; iii) la loi de 2007 sur les infractions graves (Serious Crime Act 2007) permet aux autorités publiques de divulguer des informations aux organisations de lutte contre la fraude à des fins de prévention de la fraude ([203]).

(125) Ces lois exigent explicitement que le partage d'informations soit effectué dans le respect des règles fixées par la loi DPA 2018. En outre, le collège britannique de la police a publié une pratique professionnelle autorisée concernant le partage d'informations ([204]) 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 l'homme. La conformité du partage avec le cadre juridique applicable en matière de protection des données peut bien entendu faire l'objet d'un contrôle juridictionnel ([205]).

(126) 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 ([206]). Ce type de partage concerne deux situations: 1) lorsqu'une autorité répressive en matière pénale partage des données avec une autorité répressive en matière non pénale autre qu'une agence de renseignement (par exemple, une autorité financière ou fiscale, une autorité de concurrence, un service

([198]) Article 8, paragraphe 1, de la loi de 1998 sur les droits de l'homme.

([199]) Article 36, paragraphe 3, de la loi DPA 2018.

([200]) Article 56 de la loi de 2017 sur l'économie numérique, disponible à l'adresse suivante: https://www.legislation.gov.uk/ukpga/2017/30/contents.

([201]) Article 48 de la loi de 2017 sur l'économie numérique.

([202]) 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/contents.

([203]) 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.

([204]) La pratique professionnelle agréée pour le partage d'informations est disponible à l'adresse suivante: https://www.app.college.police.uk/app-content/information-management/sharing-police-information.

([205]) Voir, par exemple, l'affaire M/the Chief Constable of Sussex Police [2019] EWHC 975 (Admin), dans laquelle la Haute Cour a été saisie pour examiner le partage de données entre la police et un partenariat pour la réduction de la criminalité d'entreprise (Business Crime Reduction Partnership – BCRP), une organisation habilitée à gérer un système d'avis d'exclusion, interdisant à certaines personnes d'entrer dans les locaux commerciaux de ses membres. La Haute Cour a examiné le partage de données, qui était effectué sur la base d'un accord ayant pour finalité la protection du public et la prévention du crime, et a finalement conclu que la majorité des aspects du partage de données étaient licites, sauf en ce qui concerne certaines informations sensibles que la police et le BRCP partageaient entre eux. Un autre exemple est l'affaire Cooper/NCA [2019] EWCA Civ 16, dans laquelle la Cour d'appel a confirmé le partage de données entre la police et l'Agence de lutte contre la grande criminalité organisée, une autorité répressive qui fait actuellement partie de l'Agence nationale de lutte contre la criminalité.

([206]) Article 36, paragraphe 4, de la loi DPA 2018.

d'aide sociale à l'enfance); 2) lorsqu'une autorité répressive en matière pénale partage des données avec une agence de renseignement. Dans la première situation, le traitement de données à caractère personnel relèvera du champ d'application du RGPD du Royaume-Uni ainsi que de la partie 2 de la loi DPA 2018. Comme précisé dans la décision XXX adoptée en vertu du règlement (UE) 2016/679, les garanties prévues par le RGPD du Royaume-Uni et par la partie 2 de la loi DPA 2018 assurent un niveau de protection essentiellement équivalent à celui assuré au sein de l'Union ([207]).

(127) Dans la seconde situation, concernant le partage de données collectées par une autorité répressive en matière pénale avec une agence de renseignement aux fins de la sauvegarde de la sécurité nationale, la base juridique autorisant ce partage est la loi de 2008 relative à la lutte contre le terrorisme, dite «loi CTA 2008» ([208]). En vertu de la loi CTA 2008, toute personne peut fournir des informations à l'un des services de renseignement en vue de l'exercice d'une des fonctions de ce service, dont celle liée à la «sécurité nationale».

(128) En ce qui concerne les conditions dans lesquelles les données peuvent être partagées aux fins de la sauvegarde de la sécurité nationale, la loi sur les services de renseignement (Intelligence Services Act) et la loi sur les services de sécurité (Security Services Act) limitent la capacité d'obtention de données des services de renseignement à ce qui est nécessaire pour s'acquitter de leurs fonctions statutaires. Les autorités compétentes qui relèvent du champ d'application de la partie 3 de la loi DPA 2018 et qui visent à partager des données avec les services de renseignement devront tenir compte d'un certain nombre de facteurs/limitations, en plus des fonctions statutaires des agences, fixées dans la loi sur les services de renseignement et la loi sur les services de sécurité ([209]). L'article 20 de la loi CTA 2008 précise que tout partage de données au titre de l'article 19 de la loi CTA 2008 doit toujours être conforme à la législation sur la protection des données, ce qui signifie que toutes les limitations et exigences prévues par la loi DPA 2018 s'appliquent. Par ailleurs, les autorités répressives et les services de renseignement sont des autorités publiques au sens de la loi de 1998 sur les droits de l'homme et doivent donc veiller à ce que leurs agissements soient conformes aux droits garantis en vertu de la CEDH, y compris son article 8. Autrement dit, ces exigences signifient que tout partage de données entre les autorités répressives et les services de renseignement est conforme à la législation sur la protection des données et à la CEDH.

(129) Le traitement, par les services de renseignement, de données à caractère personnel reçues ou obtenues auprès des autorités répressives aux fins de la sauvegarde de la sécurité nationale est soumis à un certain nombre de conditions et garanties ([210]). La partie 4 de la loi DPA 2018 s'applique à toutes les opérations de traitement effectuées par les services de renseignement ou en leur nom. Elle fixe les principes essentiels de la protection des

([207]) Décision d'exécution de la Commission constatant, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, le caractère adéquat du niveau de protection des données à caractère personnel assuré par le Royaume-Uni C(2021) 4800.

([208]) Article 19 de la loi de 2008 relative à la lutte contre le terrorisme, disponible à l'adresse suivante: https://www.legislation.gov.uk/ukpga/2008/28/section/19.

([209]) L'article 2, paragraphe 2, de la loi 1994 sur les services de renseignement (voir: https://www.legislation.gov.uk/ukpga/1994/13/contents) dispose que «[l]e chef du service de renseignement est responsable de l'efficacité de ce service et il lui incombe de veiller à ce que a) des dispositions soient en place pour s'assurer que le service de renseignement n'obtient aucune information, sauf si cela lui est nécessaire pour s'acquitter correctement de ses fonctions, et qu'il ne divulgue aucune information, sauf si cela est nécessaire i) à cette finalité; ii) aux intérêts de sécurité nationale; iii) aux fins de prévention ou de détection des infractions graves; ou iv) aux fins de toute procédure pénale; et que b) le service de renseignement ne prenne aucune mesure en vue de servir les intérêts d'un parti politique du Royaume-Uni», alors que l'article 2, paragraphe 2, de la loi de 1989 sur les services de sécurité (voir: https://www.legislation.gov.uk/ukpga/1989/5/contents) dispose que «[l]e directeur général est responsable de l'efficacité de ce service et il lui incombe de veiller à ce que a) des dispositions soient en place pour s'assurer que le service n'obtient aucune information, sauf si cela lui est nécessaire pour s'acquitter correctement de ses fonctions, et qu'il ne divulgue aucune information, sauf si cela est nécessaire à cette finalité ou aux fins de prévention ou de détection des infractions graves ou aux fins de toute procédure pénale; et que b) le service ne prenne aucune mesure en vue de servir les intérêts d'un parti politique; et que c) des dispositions convenues avec le directeur général de l'Agence nationale de lutte contre la criminalité soient en place afin de coordonner les activités du service en application de l'article 1, paragraphe 4, de la présente loi avec les activités des forces de police, de l'Agence nationale de lutte contre la criminalité et les autres autorités répressives».

([210]) Les garanties et les limitations des pouvoirs des services de renseignement sont également réglementées par la loi de 2016 sur les pouvoirs d'enquête qui, conjointement avec la loi de 2000 portant réglementation des pouvoirs d'enquête (Regulation of Investigatory Powers Act 2000) pour l'Angleterre, le pays de Galles et l'Irlande du Nord et avec la loi de 2000 portant réglementation des pouvoirs d'enquête en Écosse [Regulation of Investigatory Powers (Scotland) Act 2000] pour l'Écosse, fixe la base juridique pour l'exercice de ces pouvoirs. Ces pouvoirs ne sont toutefois pas pertinents dans le contexte du «partage ultérieur», puisqu'ils couvrent la collecte directe de données à caractère personnel par les agences de renseignement. Pour une évaluation des pouvoirs accordés aux agences de renseignement au titre de la loi sur les pouvoirs d'enquête, voir la décision d'exécution de la Commission constatant, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, le caractère adéquat du niveau de protection des données à caractère personnel assuré par le Royaume-Uni C(2021) 4800.

données (licéité, loyauté et transparence ([211]); limitation des finalités ([212]); minimisation des données ([213]); exactitude ([214]); limitation de la conservation ([215]) et sécurité ([216]), impose des conditions au traitement de données de catégories spéciales ([217]), prévoit des droits pour les personnes concernées ([218]), exige la protection des données dès la conception ([219]) et réglemente les transferts internationaux de données à caractère personnel ([220]).

(130) Parallèlement, l'article 110 de la loi DPA 2018 prévoit une dérogation à certaines dispositions énoncées dans la partie 4 de la loi DPA 2018 lorsque cette dérogation est nécessaire à la sauvegarde de la sécurité nationale. L'article 110, paragraphe 2, de la loi DPA 2018 énumère les dispositions auxquelles il peut être dérogé. Cela comprend les principes de protection des données (hormis le principe de licéité), les droits de la personne concernée, l'obligation d'informer le commissaire à l'information de toute violation de données à caractère personnel, les pouvoirs d'inspection du commissaire à l'information conformément aux obligations internationales, certains pouvoirs d'application du commissaire à l'information, les dispositions qui érigent en infraction pénale certaines violations de données à caractère personnel et les dispositions relatives aux finalités spéciales du traitement, telles que les fins journalistiques, académiques ou artistiques. Cette exemption peut être appliquée sur la base d'une analyse au cas par cas ([221]). Comme expliqué par les autorités du Royaume-Uni et tel que confirmé par la jurisprudence des tribunaux du Royaume-Uni, «a) le responsable du traitement doit tenir compte des conséquences réelles pour la sécurité ou la défense nationales s'il devait se conformer à la disposition particulière relative à la protection des données, et s'il pouvait se conformer raisonnablement aux règles habituelles sans avoir d'incidence sur la sécurité nationale ou la défense» ([222]). La question de savoir si l'exemption a été appliquée de manière appropriée est soumise à la surveillance de l'ICO ([223]).

([211]) En application de l'article 86, paragraphe 6, de la loi DPA 2018, afin d'apprécier la loyauté et la transparence du traitement, il convient de prendre en considération la méthode par laquelle les données ont été obtenues. En ce sens, l'exigence de loyauté et de transparence est satisfaite si les données sont obtenues auprès d'une personne légalement autorisée à les fournir ou tenue de le faire.

([212]) 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 ont été collectées. Conformément à l'article 87, paragraphe 3, le traitement de données à caractère personnel ultérieur compatible n'est permis que si le responsable du traitement est autorisé par la loi à traiter les données pour cette finalité et si le traitement est nécessaire et proportionné à cette finalité. Le traitement doit être considéré comme compatible lorsqu'il s'agit d'un traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, soumis à des garanties appropriées (article 87, paragraphe 4, de la loi DPA 2018).

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

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

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

([216]) 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 comprennent (mais ne s'y limitent pas) l'accès accidentel ou non autorisé aux données à caractère personnel, ou leur destruction, perte, utilisation, modification ou divulgation (article 91 de la loi DPA 2018). L'article 107 exige également que 1) chaque responsable du traitement mette en œuvre les mesures de sécurité appropriées aux risques découlant du traitement de données à caractère personnel et que 2) dans le cas d'un traitement automatisé, chaque responsable du traitement et sous-traitant mettent en œuvre des mesures de prévention ou d'atténuation reposant sur une évaluation des risques.

([217]) Article 86, paragraphe 2, point b), et annexe 10 de la loi DPA 2018.

([218]) Partie 4, chapitre 3, de la DPA 2018, notamment les droits: d'accès, de rectification et d'effacement, de s'opposer au traitement et de ne pas faire l'objet d'une décision automatisée, d'intervenir dans la prise de décision automatisée et d'être informé de la décision. Par ailleurs, le responsable du traitement est tenu de fournir à la personne concernée les informations relatives au traitement de ses données à caractère personnel.

([219]) Article 103 de la loi DPA 2018.

([220]) Article 109 de la loi DPA 2018. Les transferts de données à caractère personnel vers des organisations internationales ou des pays en dehors du Royaume-Uni sont possibles si ces transferts constituent une mesure nécessaire et proportionnée prise aux fins des fonctions statutaires du responsable du traitement, ou à d'autres fins prévues par des articles particuliers de la loi de 1989 sur les services de sécurité et de la loi de 1994 sur les services de renseignement (Intelligence Services Act 1994).

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

([222]) Cadre explicatif du Royaume-Uni pour la discussion relative à l'adéquation, section H: Cadre relatif à la protection de données et aux pouvoirs d'enquêtes dans le contexte de sécurité nationale (National Security Data Protection and Investigatory Powers Framework), pages 15-16, disponible à l'adresse suivante: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf. Voir également l'affaire Baker/Secretary of State (voir la note de bas de page ci-dessus 220), dans laquelle le tribunal a invalidé un certificat de sécurité nationale délivré par le ministre de l'intérieur et confirmant l'application de la dérogation de sécurité nationale, considérant qu'aucune raison ne justifiait une exception générale à l'obligation de donner suite aux demandes d'accès et que permettre cette exception en toutes circonstances sans une analyse au cas par cas excédait ce qui était nécessaire et proportionné à la sauvegarde de la sécurité nationale.

([223]) Voir le protocole d'accord entre l'ICO et l'UKIC (UK Intelligence Community – communauté de renseignement du Royaume-Uni), selon lequel «[l]orsque l'ICO recevra une réclamation d'une personne concernée, il s'assurera que la question aura été traitée comme il se doit, et, le cas échéant, que la dérogation aura bien été invoquée de manière appropriée» (point 16 du protocole d'accord conclu entre le bureau du commissaire à l'information et la communauté de renseignement du Royaume-Uni, disponible à l'adresse suivante: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf).

(131) De plus, en ce qui concerne la possibilité de limiter l'un des droits susmentionnés aux fins de la protection de la «sécurité nationale», l'article 79 de la DPA 2018 prévoit la possibilité pour un responsable du traitement de déposer une demande de certificat signé par un ministre ou le procureur général attestant qu'une limitation de ces droits est, ou a été à un moment donné, une mesure nécessaire et proportionnée pour sauvegarder la sécurité nationale. ([224]) Le gouvernement du Royaume-Uni a publié des orientations relatives aux certificats de sécurité nationale au titre de la loi DPA 2018, qui soulignent notamment que toute limitation des droits de la personne concernée pour la sauvegarde de la sécurité nationale doit être nécessaire et proportionnée ([225]). Tous les certificats de sécurité nationale doivent être publiés sur le site internet de l'ICO ([226]).

(132) Le certificat devrait être valable pour une durée déterminée n'excédant pas cinq ans, de manière à être régulièrement révisé par le pouvoir exécutif ([227]). 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 ([228]).

(133) Il est important de noter que les certificats de sécurité nationale ne constituent pas un motif supplémentaire de restreindre les droits en matière de protection des données pour des raisons de sécurité nationale. En d'autres termes, le responsable du traitement ou le sous-traitant ne peut faire valoir un certificat que s'il est arrivé à la conclusion qu'il est nécessaire d'invoquer la dérogation de sécurité nationale, qui doit s'appliquer au cas par cas. 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 ([229]).

(134) Toute personne directement concernée par la délivrance du certificat peut introduire un recours auprès du tribunal supérieur ([230]) contre le certificat ([231]) ou, lorsque le certificat définit les données au moyen d'une description générale, remettre en question l'application du certificat à certaines données ([232]).

(135) Le tribunal examinera la décision de délivrer un certificat et déterminera s'il existait des motifs raisonnables de le délivrer ([233]). Il peut étudier un large éventail de questions, y compris la nécessité, la proportionnalité et la licéité, en tenant compte de l'incidence sur les droits des personnes concernées et en équilibrant la nécessité de sauvegarder 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 ([234]).

([224]) La loi DPA 2018 a révoqué la possibilité d'émettre un certificat en vertu de l'article 28, paragraphe 2, de la loi de 1998 sur la protection des données. Toutefois, la possibilité d'émettre d'«anciens certificats» persiste dans la mesure où il existe une possibilité de recours historique en vertu de la loi de 1998 (voir le paragraphe 17 de la partie 5 de l'annexe 20 de la loi DPA 2018). Toutefois, cette possibilité semble très rare et ne s'applique que dans des cas limités, notamment lorsqu'une personne concernée introduit un recours contre l'application de l'exemption concernant la sécurité nationale pour un traitement effectué par une autorité publique sous l'empire de la loi de 1998. Il convient de noter que dans ces cas, l'article 28 de la loi DPA 1998 s'applique intégralement, ce qui inclut la possibilité pour la personne concernée d'introduire un recours contre le certificat. À l'heure actuelle, aucun certificat de sécurité nationale n'a été émis en vertu de la loi DPA 1998.

([225]) 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

([226]) Conformément à l'article 130 de la loi DPA 2018, l'ICO peut décider de ne pas publier tout ou partie du texte du certificat dans le cas où cette publication serait contraire à l'intérêt de la sécurité nationale ou à l'intérêt public ou serait susceptible de compromettre la sécurité d'une personne. Dans de tels cas, l'ICO publie toutefois le fait que le certificat a été émis.

([227]) Point 15 des orientations du gouvernement du Royaume-Uni sur les certificats de sécurité nationale, voir la note de bas de page n° 225.

([228]) Point 5 des orientations du gouvernement du Royaume-Uni sur les certificats de sécurité nationale, voir la note de bas de page n° 225.

([229]) 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 implique que le service de renseignement serait tenu de prouver à l'ICO que, lorsqu'il invoque la dérogation, il a pris en considération les circonstances spécifiques de la situation. L'ICO publie également un registre des certificats de sécurité nationale, qui est disponible à l'adresse suivante: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/.

([230]) 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.

([231]) Article 111, paragraphe 3, de la loi DPA 2018.

([232]) Article 111, paragraphe 5, de la loi DPA 2018.

([233]) Dans l'affaire Baker/Secretary of State (voir la note de bas de page n° 221, le tribunal compétent en matière d'informations a invalidé un certificat de sécurité nationale délivré par le ministre de l'intérieur, considérant qu'aucune raison ne justifiait une exception générale à l'obligation de donner suite aux demandes d'accès et que permettre cette exception en toutes circonstances sans une analyse au cas par cas excédait ce qui était nécessaire et proportionné à la sauvegarde de la sécurité nationale.

([234]) Point 25 des orientations du gouvernement du Royaume-Uni sur les certificats de sécurité nationale, voir la note de bas de page n° 225.

(136) 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 ([235]) 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. 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») ([236]). Les dérogations sur la base du préjudice ne peuvent être invoquées que tant que l'application des dispositions de protection de données énumérées serait susceptible de nuire aux intérêts spécifiques concernés. Le fait de recourir à une dérogation doit en conséquence être justifié en précisant le préjudice concerné qui pourrait se produire dans le cas en question. Les dérogations sur la base de la catégorie ne peuvent être invoquées qu'en ce qui concerne la catégorie d'informations spécifique et circonscrite pour laquelle la dérogation est accordée. En ce qui concerne leurs objectifs et leurs effets, ces dérogations sont similaires à plusieurs des dérogations énoncées dans le RGPD du Royaume-Uni (au titre de l'annexe 2 de la loi DPA 2018) qui, elles-mêmes, reflètent celles prévues par l'article 23 du RGPD.

(137) 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.

(138) Le commissaire à l'information surveille le traitement de données à caractère personnel effectué par les services de renseignement en vertu de la partie 4 de la loi DPA 2018 ([237]).

(139) 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. Les missions comprennent notamment, mais sans s'y limiter, la surveillance et le contrôle de l'application de la partie 4 de la loi DPA 2018, la sensibilisation du public, la dispense de conseils au Parlement, au gouvernement et à d'autres institutions au sujet des mesures législatives et administratives, la sensibilisation des responsables du traitement et des sous-traitants aux obligations qui leur incombent, la fourniture d'informations à une personne concernée sur l'exercice de ses droits, et la conduite d'enquêtes.

(140) En ce qui concerne la partie 3 de la loi DPA 2018, le commissaire dispose de compétences pour notifier aux responsables du traitement une violation alléguée, avertir qu'une opération de traitement est susceptible d'enfreindre les règles et rappeler à l'ordre lorsque la violation est confirmée. Il peut également émettre des avis d'exécution et de sanction en cas de violations de certaines dispositions de ladite loi ([238]). Néanmoins, à la différence des autres parties de la loi DPA 2018, le commissaire ne peut pas adresser d'avis d'évaluation à un organisme de sécurité nationale ([239]).

(141) En outre, l'article 110 de la loi DPA 2018 prévoit une exception à l'utilisation de certains pouvoirs du commissaire lorsque cela est requis aux fins de la sauvegarde de la sécurité nationale. Cela comprend le pouvoir du commissaire d'émettre des avis (de tout type) en vertu de la loi DPA (avis d'information, avis d'évaluation, avis d'exécution et avis de sanction), le pouvoir de mener des inspections conformément aux obligations internationales, les pouvoirs

([235]) Cela comprend: i) les 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) les droits des personnes concernées; et iii) les obligations relatives à la notification des violations à l'ICO.

([236]) 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 notes d'examen. Les dérogations «sur la base du préjudice» concernent les questions suivantes: i) la prévention ou la détection des infractions pénales; l'arrestation et la poursuite des auteurs d'infractions; ii) l'immunité parlementaire; iii) le déroulement des 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 du Royaume-Uni pour la discussion relative à l'adéquation, section H: Sécurité nationale, p. 13, voir la note de bas de page n° 222.

([237]) Article 116 de la loi DPA 2018.

([238]) Il ressort d'une lecture combinée de l'article 149, paragraphe 2, et de l'article 155 de la loi DPA 2018, que les avis d'exécution et de sanction peuvent être adressés à un responsable du traitement ou sous-traitant en cas de violations du chapitre 2 de la partie 4 de la loi DPA 2018 (principes de traitement), d'une disposition de la partie 4 de la loi DPA 2018 conférant des droits à une personne concernée, d'une obligation d'informer le commissaire d'une violation de données à caractère personnel en application de l'article 108 de la loi DPA 2018 et des principes relatifs aux transferts de données à caractère personnel vers des pays tiers, des pays non liés par la convention et des organisations internationales énoncés à l'article 109 de la loi DPA 2018. (Pour plus de détails sur les avis d'exécution et de sanction, voir les considérants 102 et 103.)

([239]) En vertu de l'article 147, paragraphe 6, de la loi DPA 2018, le commissaire à l'information ne peut pas adresser d'avis d'évaluation à un organisme visé à l'article 23, paragraphe 3, de la loi de 2000 sur la liberté d'information (Freedom of Information Act 2000). Il s'agit notamment du service de sécurité (MI5), du service secret de renseignement (MI6) et du quartier général des communications.

d'accès et d'inspection et les règles relatives aux infractions ([240]). Comme expliqué au considérant 136, ces exceptions ne s'appliqueront, au cas par cas, que si elles constituent une mesure nécessaire et proportionnée. L'application de ces dérogations peut faire l'objet d'un contrôle juridictionnel ([241]).

(142) L'ICO et les services de renseignement du Royaume-Uni ont signé un protocole d'accord ([242]) fixant un cadre pour la coopération sur un certain nombre de questions, dont les notifications de violation de données à caractère personnel et le traitement des réclamations de personnes concernées. En particulier, ce protocole prévoit que, lorsqu'il reçoit une réclamation, l'ICO évaluera si une dérogation de sécurité nationale a bien été invoquée de manière appropriée. Les réponses aux demandes faites par l'ICO dans le contexte de l'examen des réclamations individuelles doivent être apportées dans un délai de 20 jours ouvrés par les orientations du gouvernement du Royaume-Uni sur les certificats de sécurité nationale, en application de la loi sur la protection des données, au moyen de canaux sécurisés adéquats dans le cas où des renseignements classifiés sont concernés. Du mois d'avril 2018 à ce jour, l'ICO a reçu 21 réclamations de la part de particuliers concernant les services de renseignement. Chaque réclamation a été évaluée et l'issue a été notifiée à la personne concernée ([243]).

(143) De plus, le Comité de renseignement et de sécurité (Intelligence and Security Committee – ISC) exerce un contrôle parlementaire sur le traitement de données par les agences de renseignement. Le Comité trouve sa base légale dans la loi de 2013 sur la justice et la sécurité (Justice and Security Act 2013), dite «loi JSA 2013» ([244]). La loi institue l'ISC comme une commission du Parlement du Royaume-Uni. L'ISC est composé de membres appartenant à l'une ou l'autre Chambre du Parlement et nommés par le Premier ministre après consultation du chef de l'opposition ([245]). L'ISC est tenu de présenter un rapport annuel devant le Parlement sur l'exercice de ses fonctions et d'autres rapports qu'il estime pertinents ([246]).

(144) Depuis 2013, l'ISC est investi de pouvoirs accrus, dont la supervision des activités opérationnelles des services de sécurité. Conformément à l'article 2 de la loi JSA 2013, l'ISC a pour mission de superviser les dépenses, l'administration, la politique et les opérations des agences de sécurité nationale. La loi JSA 2013 précise que l'ISC est habilité à mener des enquêtes sur des questions opérationnelles lorsqu'elles ne concernent pas des opérations en

([240]) Les dispositions pouvant faire l'objet d'une dérogation sont les suivantes: l'article 108 (informer le commissaire d'une violation de données à caractère personnel), l'article 119 (mener des inspections conformément aux obligations internationales); les articles 142 à 154 et l'annexe 15 (avis du commissaire et pouvoirs d'accès et d'inspection); et les articles 170 à 173 (infractions relatives aux 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.

([241]) Voir exemple l'affaire Baker/Secretary of State for the Home Department (voir la note de bas de page n° 221).

([242]) Protocole d'accord entre l'ICO et la communauté de renseignement du Royaume-Uni, voir la note de bas de page n° 231.

([243]) Dans sept de ces cas, l'ICO a conseillé à l'auteur de la réclamation de faire part de ses inquiétudes auprès du responsable du traitement (il s'agit du cas où une personne a exprimé ses inquiétudes auprès de l'ICO, mais qu'elle aurait d'abord dû le faire auprès du responsable du traitement). Dans l'un de ces cas, l'ICO a dispensé des conseils généraux au responsable du traitement (il s'agit du cas où les agissements du responsable du traitement ne semblaient pas avoir enfreint la législation, mais où une amélioration des pratiques aurait pu éviter la communication des préoccupations à l'ICO). Dans les 13 autres cas, aucune mesure n'était requise de la part du responsable du traitement (il s'agit de cas où les préoccupations soulevées par la personne relevaient bien de la loi de 2018 sur la protection des données, car elles concernaient le traitement de données à caractère personnel, mais où il ressortait des informations fournies que le responsable du traitement ne semblait pas avoir enfreint la législation).

([244]) Comme expliqué par les autorités du Royaume-Uni, la loi JSA a élargi les attributions de l'ISC pour y inclure un rôle de supervision de la communauté de renseignement au-delà des trois agences et permettre la supervision rétrospective des activités opérationnelles des agences sur des questions d'intérêt national majeur.

([245]) Article 1er de la loi JSA 2013. Les ministres ne sont pas éligibles pour devenir membres. Les membres occupent leur poste au sein de l'ISC pendant la durée de la législature du Parlement au cours de laquelle ils ont été nommés. La Chambre qui les a nommés peut les destituer par voie de résolution, ou ils peuvent être révoqués s'ils cessent d'être membres du Parlement, ou s'ils deviennent ministres. Un membre peut également démissionner.

([246]) Les rapports et les déclarations du Comité sont disponibles à l'adresse suivante: http://isc.independent.gov.uk/committee-reports. 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://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf), dans lequel il étudiait le cadre juridique relatif aux techniques de surveillance employées par les agences de renseignement, et a émis une série de recommandations qui ont été examinées par la suite et incorporées dans le projet de loi sur les pouvoirs d'enquête (Investigatory Powers Bill), converti en loi – IPA 2016. La réponse du gouvernement à ce rapport relatif à la vie privée et à 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.

cours ([247]). Le protocole d'accord conclu entre le Premier ministre et l'ISC ([248]) définit en détail les éléments à prendre en considération pour déterminer si une activité fait ou non partie d'une opération en cours ([249]). L'ISC peut également être invité par le Premier ministre à enquêter sur des opérations en cours et peut examiner les informations fournies de plein gré par les agences.

(145) En vertu de l'annexe 1 de la loi JSA 2013, l'ISC peut demander aux dirigeants de l'un des trois services de renseignement de divulguer toute information. L'agence doit rendre ces informations disponibles, à moins que le secrétaire d'État n'y oppose son veto ([250]). Les autorités du Royaume-Uni ont expliqué qu'en pratique, très peu d'informations ne sont pas communiquées à l'ISC ([251]).

(146) Tout d'abord, en ce qui concerne la réparation, une personne concernée peut, conformément à l'article 165, paragraphe 2, de la loi DPA 2018, introduire une réclamation auprès de l'ICO si elle considère qu'il y a eu violation de la partie 4 de la loi DPA 2018 quant aux données à caractère personnel la concernant, y compris toute utilisation abusive des dérogations de sécurité nationale et des limitations.

(147) En outre, au titre de la partie 4 de la loi DPA 2018, les personnes ont le droit de solliciter auprès de la Haute Cour (ou de la Cour de session en Écosse) une ordonnance exigeant du responsable du traitement qu'il respecte le droit d'accès aux données ([252]), le droit de s'opposer à leur traitement ([253]) ainsi que le droit de rectification et le droit à l'effacement.

(148) Les personnes ont également le droit de demander une indemnisation pour un préjudice subi en raison de la violation d'une exigence énoncée dans la partie 4 de la loi DPA 2018 par le responsable du traitement ou un sous-traitant ([254]). Le préjudice comprend aussi bien la perte financière que le préjudice n'entraînant aucune perte financière, tel que la détresse ([255]).

(149) Enfin, une personne peut introduire une réclamation auprès du tribunal chargé des pouvoirs d'enquête (Investigatory Powers Tribunal), dit «IPT», pour tout comportement de la part ou au nom des agences de renseignement du Royaume-Uni ([256]). L'IPT est institué par la loi de 2000 portant réglementation des pouvoirs d'enquête pour l'Angleterre, le pays de Galles et l'Irlande du Nord et la loi de 2000 portant réglementation des pouvoirs d'enquête (Écosse) pour l'Écosse («loi RIPA 2000») et est indépendant du pouvoir exécutif ([257]). En vertu de l'article 65 de la loi RIPA 2000, les membres de l'IPT sont nommés par la Reine pour une durée de cinq ans.

(150) Un membre du tribunal peut être démis de ses fonctions par la Reine à la suite d'une requête ([258]) émise par les deux Chambres du Parlement ([259]).

(151) Afin d'engager une action en justice devant l'IPT («qualité pour agir»), en vertu de l'article 65 de la loi RIPA 2000, une personne doit croire i) que le comportement d'un service de renseignement concernait sa personne, l'un de ses biens, toute communication qu'elle a envoyée ou reçue, ou qui lui est destinée, ou son utilisation d'un service postal, d'un service de télécommunications ou d'un système de télécommunications ([260]), et ii) que le comportement a eu lieu

([247]) Article 2 de la loi JSA 2013.
([248]) Protocole d'accord conclu entre le Premier ministre et l'ISC, disponible à l'adresse suivante: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf
([249]) Point 14 du protocole d'accord entre le Premier ministre et l'ISC, voir la note de bas de page n° 248.
([250]) Le secrétaire d'État ne peut opposer son veto à la divulgation d'informations que pour deux motifs: les informations sont sensibles et ne devraient pas être divulguées à l'ISC à des fins de sauvegarde de la sécurité nationale; ou il s'agit d'informations d'une nature telle que, si le secrétaire d'État était invité à les produire devant une commission d'enquête départementale de la Chambre des communes, il estimerait (pour des motifs qui ne se limitent pas à la sauvegarde de la sécurité nationale) qu'il convient de ne pas le faire [annexe 1, point 4 2), de la loi JSA 2013].
([251]) Cadre explicatif du Royaume-Uni – section H: Sécurité nationale, p. 43.
([252]) Article 94, paragraphe 11, de la loi DPA 2018.
([253]) Article 99, paragraphe 4, de la loi DPA 2018.
([254]) L'article 169 de la loi DPA 2018 permet à «une personne qui subit un préjudice en raison de la violation d'une exigence de la législation sur la protection des données» d'introduire des réclamations.
([255]) Article 169, paragraphe 5, de la loi DPA 2018.
([256]) Voir l'article 65, paragraphe 2, point b), de la loi RIPA.
([257]) Conformément à l'annexe 3 de la loi RIPA 2000, les membres doivent justifier d'une expérience spécifique dans le domaine judiciaire et leur mandat peut être renouvelé.
([258]) Sur la notion de requête, voir la note de bas de page n° 183.
([259]) Annexe 3, point 1 5), de la loi RIPA 2000.
([260]) Article 65, paragraphe 4, de la loi RIPA 2000.

dans des «circonstances contestables» ([261]) ou qu'il s'agit d'un comportement «de la part ou au nom des services de renseignement» ([262]). Étant donné que ce critère de «conviction» en particulier a été interprété de manière assez large ([263]), la saisine du tribunal nécessite une qualité pour agir relativement faible.

(152) Lorsqu'un tribunal examine une réclamation qui lui est adressée, il a pour devoir d'enquêter pour déterminer si les personnes contre qui toute allégation est formulée dans la réclamation ont agi à l'égard de l'auteur de la réclamation, ainsi que d'enquêter sur l'autorité qui aurait commis des violations et sur la question de savoir si le comportement allégué a eu lieu ([264]). Lorsque le tribunal est saisi de toute procédure, il doit appliquer les mêmes principes pour prendre sa décision dans le cadre de cette procédure que ceux qu'appliquerait une juridiction pour examiner une demande de contrôle juridictionnel ([265]).

(153) Le tribunal est tenu d'informer l'auteur de la réclamation si une décision a été prise en sa faveur ou non ([266]). En vertu de l'article 67, paragraphes 6 et 7, de la loi RIPA 2000, le tribunal est habilité à rendre des ordonnances provisoires et à octroyer des indemnités ou à rendre toute autre ordonnance qu'il juge appropriée ([267]). Conformément à l'article 67A de la loi RIPA 2000, une décision du tribunal peut faire l'objet d'un recours, sous réserve de l'autorisation accordée par le tribunal ou la cour d'appel compétente.

(154) Plus particulièrement, les personnes peuvent introduire une réclamation (et obtenir réparation) auprès de l'IPT si elles estiment qu'une autorité publique a agi (ou propose d'agir) d'une manière incompatible avec les droits garantis par la CEDH, y compris le droit au respect de la vie privée et à la protection des données, et, partant, d'une manière illicite en vertu de l'article 6, paragraphe 1, de la loi de 1998 sur les droits de l'homme. L'IPT s'est vu attribuer la compétence juridictionnelle exclusive pour toutes les réclamations relevant de la loi sur les droits de l'homme et concernant les agences de renseignement. Cela signifie, comme l'a relevé la Haute Cour, que «la question de savoir s'il y a eu violation de la loi sur les droits de l'homme dans les faits d'une affaire spécifique peut, en principe, être soulevée et jugée par un tribunal indépendant qui peut avoir accès à tous les documents pertinents, y compris les documents secrets. […] Nous gardons également à l'esprit que, dans ce contexte, l'IPT peut désormais faire lui-même l'objet d'un recours devant une cour d'appel appropriée (il s'agirait de la Cour d'appel en Angleterre et au pays de Galles); et que la Cour suprême a récemment tranché que l'IPT peut en principe faire l'objet d'un contrôle juridictionnel: voir l'affaire R (Privacy International)/Investigatory Powers Tribunal [2019] UKSC 22; [2019] 2 WLR 1219» ([268]). Si l'IPT juge tout acte d'une autorité publique comme étant illicite, il est habilité, en vertu de ses pouvoirs, à accorder toute réparation ou tout recours, ou à émettre une ordonnance dans la mesure où il estime cela juste et approprié ([269]).

([261]) De telles circonstances font référence au comportement d'autorités publiques ayant lieu en vertu de leur autorité (par exemple la délivrance d'un mandat, d'une autorisation/d'un avis pour l'acquisition de communications, etc.), ou si les circonstances sont telles (qu'il y ait une telle autorité ou non) qu'il n'aurait pas été approprié que le comportement ait lieu sans elle, ou au moins sans qu'il y ait eu un examen sérieux visant à déterminer si cette autorité devrait être sollicitée. Le comportement autorisé par un commissaire judiciaire (Judicial Commissioner) est considéré comme ayant eu lieu dans des circonstances contestables [article 65 (7ZA) de la loi RIPA 2000] alors que les autres comportements qui ont lieu avec l'autorisation d'une personne exerçant une fonction judiciaire sont considérés comme n'ayant pas eu lieu dans des circonstances contestables (article 65, paragraphes 7 et 8, de la loi RIPA 2000).

([262]) D'après les informations fournies par les autorités du Royaume-Uni, vu les critères peu contraignants requis pour introduire une réclamation, il est fréquent que l'enquête du tribunal révèle que l'auteur de la réclamation n'a, en réalité, jamais fait l'objet d'une enquête menée par une autorité publique. Le dernier rapport statistique de l'IPT précise qu'en 2016, le tribunal a reçu 209 réclamations. 52 % ont été considérées comme fantaisistes ou vexatoires et 25 % d'entre elles n'ont donné lieu à «aucune décision». Selon les explications des autorités du Royaume-Uni, cela signifie soit qu'il n'y a eu aucun recours à un pouvoir dissimulé ou une activité dissimulée à l'égard de l'auteur de la réclamation, soit que des techniques dissimulées ont été employées et que le tribunal a conclu que l'activité était licite. Par ailleurs, 11 % de ces réclamations ne relevaient pas de la compétence de la juridiction, ont été retirées ou n'étaient pas valides, 5 % ont été écartées en raison de leur caractère tardif et, pour 7 % d'entre elles, l'auteur de la réclamation a obtenu gain de cause. 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.

([263]) Voir l'affaire Human Rights Watch/Secretary of State [2016] UKIPTrib15_165-CH. Dans cette situation, l'IPT, en se référant à la jurisprudence de la CEDH, a estimé que le critère approprié en ce qui concerne la conviction qu'un comportement relevant de l'article 68, paragraphe 5, de la loi RIPA 2000 a été exercé par ou au nom de l'un des services de renseignement, est de déterminer si cette conviction est fondée. Cela comprend le fait qu'une personne ne peut prétendre être victime d'une violation entraînée par la simple existence de mesures secrètes ou d'une législation permettant des mesures secrètes que si elle est en mesure de démontrer qu'en raison de sa situation personnelle, elle risque potentiellement d'être soumise à de telles mesures (voir l'affaire Human Rights Watch/Secretary of State, point 41).

([264]) Article 67, paragraphe 3, de la loi RIPA 2000.

([265]) Article 67, paragraphe 2, de la loi RIPA 2000.

([266]) Article 68, paragraphe 4, de la loi RIPA 2000.

([267]) Il peut s'agir d'une ordonnance exigeant la destruction de tout registre d'information détenu par une autorité publique concernant une personne.

([268]) Haute Cour de justice, Liberty, [2019] EWHC 2057 (Admin), point 170.

([269]) Article 8, paragraphe 1, de la loi de 1998 sur les droits de l'homme.

(155) Après avoir épuisé toutes les voies de recours nationales, une personne peut demander réparation devant la Cour européenne des droits de l'homme pour violation des droits garantis par la CEDH, dont le droit au respect de la vie privée et le droit à la protection des données.

(156) Il découle de ce qui précède que le partage par les autorités répressives en matière pénale du Royaume-Uni de données transférées au titre de la présente décision avec d'autres autorités publiques, dont les agences de renseignement, est encadré par des limitations et des conditions garantissant que ce partage ultérieur sera nécessaire et proportionné et soumis à des garanties spécifiques de protection des données en vertu de la loi DPA 2018. En outre, le traitement de données par les autorités publiques en question est surveillé par des organismes indépendants et les personnes concernées ont à leur disposition des voies de recours efficaces.

3. **CONCLUSIONS**

(157) La Commission estime que la partie 3 de la loi DPA 2018 garantit un niveau de protection des données à caractère personnel transférées, à des fins répressives, des autorités compétentes de l'Union vers les autorités compétentes du Royaume-Uni, qui est essentiellement équivalent à celui garanti par la directive (UE) 2016/680.

(158) De plus, la Commission estime que, pris dans leur ensemble, les mécanismes de surveillance et les voies de recours prévus dans le droit du Royaume-Uni permettent de détecter 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.

(159) Enfin, sur la base des informations disponibles concernant l'ordre juridique du Royaume-Uni, la Commission considère que toute atteinte aux droits fondamentaux des personnes dont les données à caractère personnel sont transférées de l'Union européenne vers le Royaume-Uni par des autorités publiques du Royaume-Uni à des fins d'intérêt public, y compris dans le contexte du partage de données à caractère personnel entre des autorités répressives et d'autres autorités publiques, telles que les organismes de sécurité nationale, sera limitée à ce qui est strictement nécessaire pour atteindre l'objectif légitime visé et qu'il existe une protection juridique effective contre les atteintes de cette nature.

(160) En conséquence, il convient de décider que le Royaume-Uni assure un niveau de protection adéquat au sens de l'article 36, paragraphe 2, de la directive (UE) 2016/680, interprété à la lumière de la charte des droits fondamentaux.

(161) Cette conclusion repose tant sur le régime national pertinent du Royaume-Uni que sur les engagements internationaux du Royaume-Uni, en particulier son adhésion à la convention européenne des droits de l'homme et le fait qu'il se soumette à la juridiction de la Cour européenne des droits de l'homme. Le respect indéfectible de ces obligations internationales est donc un élément particulièrement important de l'évaluation sur laquelle se fonde la présente décision.

4. **EFFETS DE LA PRÉSENTE DÉCISION ET ACTION DES AUTORITÉS CHARGÉES DE LA PROTECTION DES DONNÉES**

(162) 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.

(163) En conséquence, une décision d'adéquation de la Commission adoptée en vertu de l'article 36, paragraphe 3, de la directive (UE) 2016/680, a un caractère contraignant pour tous les organes des États membres destinataires, y compris leurs autorités de contrôle 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 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.

(164) Parallèlement, il convient de rappeler que, en vertu de l'article 47, paragraphe 5, de la directive (UE) 2016/680, et ainsi que la Cour de justice l'a expliqué dans l'arrêt Schrems, lorsqu'une autorité chargée de la protection des données met en cause, notamment après avoir été saisie d'une réclamation, la compatibilité d'une décision d'adéquation de la Commission avec la protection des droits fondamentaux que constituent le respect de la vie privée et la protection des données, le droit national doit prévoir des voies de recours lui permettant de faire valoir ces griefs devant les juridictions nationales, qui pourraient être amenées à procéder à un renvoi préjudiciel devant la Cour de justice ([270]).

([270]) Arrêt Schrems, point 65.

5. SUIVI, SUSPENSION, ABROGATION OU MODIFICATION DE LA PRÉSENTE DÉCISION

(165) Conformément à l'article 36, paragraphe 4, de la directive (UE) 2016/680, 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'occurrence, puisque le Royaume-Uni dirigera, appliquera et fera appliquer un nouveau régime de protection des données qui ne sera plus soumis au droit de l'Union et qui sera susceptible d'évoluer. À cet égard, une attention particulière sera accordée à l'application des règles britanniques en matière des transferts de données à caractère personnel vers des pays tiers, notamment par la conclusion de conventions internationales, à l'incidence que ces transferts pourraient avoir sur le niveau de protection conféré aux données transférées au regard de la présente décision, ainsi qu'à l'efficacité de l'exercice des droits individuels dans les domaines couverts par la présente décision. Parmi d'autres éléments, la Commission fondera son suivi sur les évolutions de la jurisprudence et sur la surveillance exercée par l'ICO et par d'autres organismes indépendants.

(166) Afin de faciliter ce suivi, les autorités du Royaume-Uni sont invitées à informer sans délai et régulièrement la Commission de toute modification de fond apportée à l'ordre juridique britannique 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 particulier en ce qui concerne les éléments mentionnés au considérant 165.

(167) En outre, afin de permettre à la Commission d'accomplir efficacement sa mission de suivi, les États membres devraient l'informer de toute mesure pertinente prise par les autorités nationales chargées de la protection des données, en particulier en ce qui concerne les questions ou les plaintes des personnes concernées de l'Union européenne au sujet du transfert de données à caractère personnel des autorités compétentes de l'Union vers les autorités compétentes du Royaume-Uni. La Commission devrait également être informée de tout élément indiquant que les actions des autorités publiques du Royaume-Uni compétentes pour la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière, y compris de tout organisme de surveillance, n'assurent pas le niveau de protection requis.

(168) Lorsque des informations disponibles, en particulier les informations résultant 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 sans délai les autorités compétentes du Royaume-Uni et demander que des mesures appropriées soient prises dans un délai bien défini, qui ne peut excéder trois mois. Si nécessaire, cette période peut être prolongée pour une durée bien définie, en tenant compte de la nature du problème à régler ou des mesures à prendre.

(169) Si, à l'expiration de ce délai défini, les autorités compétentes du Royaume-Uni échouent à prendre ces mesures ou à démontrer autrement de manière satisfaisante que la présente décision reste fondée sur un niveau de protection adéquat, la Commission lancera la procédure visée à l'article 58, paragraphe 2, de la directive (UE) 2016/680, en vue de suspendre partiellement ou complètement ou d'abroger la présente décision.

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

(171) Pour des raisons d'urgence impérieuses dûment justifiées, la Commission recourra à la possibilité d'adopter des actes d'exécution suspendant, abrogeant ou amendant la présente décision, qui seraient immédiatement applicables, conformément à la procédure visée à l'article 58, paragraphe 3, de la directive (UE) 2016/680.

6. DURÉE ET RENOUVELLEMENT DE LA PRÉSENTE DÉCISION

(172) Il convient de noter que, à la fin de la période de transition prévue par l'accord de retrait et dès que la disposition transitoire visée à l'article 782 de l'accord de commerce et de coopération UE-Royaume-Uni cessera d'être applicable, le Royaume-Uni dirigera, appliquera et fera appliquer un nouveau régime de protection des données, autre que celui qui était en place lorsque le Royaume-Uni était lié par le droit de l'Union européenne. Cela peut notamment impliquer des amendements ou des modifications du cadre de protection des données évalué dans la présente décision, de même que d'autres évolutions pertinentes.

(173) Il convient donc de prévoir que la présente décision sera applicable pour une durée de quatre ans à compter de son entrée en vigueur.

(174) Lorsque des informations particulières résultant du suivi de la présente décision révèlent que les conclusions relatives à l'adéquation du niveau de protection assuré par le Royaume-Uni sont toujours justifiées en fait et en droit, la Commission devrait, au plus tard six mois avant que la présente décision ne cesse de s'appliquer, lancer la procédure de modification de la présente décision en étendant sa portée dans le temps, en principe, pour une durée supplémentaire de quatre ans. Tout acte d'exécution portant modification de la présente décision doit être adopté conformément à la procédure mentionnée à l'article 58, paragraphe 2, de la directive (UE) 2016/680.

7. **CONSIDÉRATIONS FINALES**

(175) Le comité européen de la protection des données a publié son avis ([271]), dont il a été tenu compte dans l'élaboration de la présente décision.

(176) Les mesures prévues dans la présente décision sont conformes à l'avis du comité institué par l'article 58 de la directive (UE) 2016/680.

(177) Conformément à l'article 6 *bis* du protocole n° 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, l'Irlande n'est pas liée par les règles fixées dans la directive (UE) 2016/680, et donc dans la présente décision d'exécution, concernant le traitement de données à caractère personnel par les États membres dans l'exercice d'activités qui relèvent du champ d'application du chapitre 4 ou 5 du titre V de la troisième partie du traité sur le fonctionnement de l'Union européenne, lorsque l'Irlande n'est pas liée par les règles qui régissent des formes de coopération judiciaire en matière pénale ou de coopération policière dans le cadre desquelles les dispositions fixées sur la base de l'article 16 du traité sur le fonctionnement de l'Union européenne doivent être respectées. En outre, en vertu de la décision d'exécution (UE) 2020/1745 du Conseil ([272]), la directive (UE) 2016/680 sera mise en œuvre et appliquée provisoirement en Irlande à partir du 1er janvier 2021. L'Irlande est donc liée par la présente décision d'exécution, dans les mêmes conditions que celles relatives à l'application de la directive (UE) 2016/680 en Irlande, énoncées dans la décision d'exécution (UE) 2020/1745, en ce qui concerne l'acquis de Schengen auquel elle participe.

(178) Conformément aux articles 2 et 2 *bis* du protocole n° 22 sur la position du Danemark, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Danemark n'est pas lié par les règles fixées dans la directive (UE) 2016/680, et donc dans la présente décision d'exécution, ni soumis à leur application, lorsqu'elles concernent le traitement de données à caractère personnel par les États membres dans l'exercice d'activités qui relèvent du champ d'application du chapitre 4 ou 5 du titre V de la troisième partie du traité sur le fonctionnement de l'Union européenne. Toutefois, étant donné que la directive (UE) 2016/680 développe l'acquis de Schengen, le Danemark, conformément à l'article 4 de ce protocole, a notifié le 26 octobre 2016 sa décision de mettre la directive (UE) 2016/680 en œuvre. Le Danemark est donc tenu, en application du droit international, de mettre en œuvre la présente décision d'exécution.

(179) En ce qui concerne l'Islande et la Norvège, la présente décision d'exécution constitue un développement des dispositions de l'acquis de Schengen au sens de l'accord conclu par le Conseil de l'Union européenne, la République d'Islande et le Royaume de Norvège sur l'association de ces deux États à la mise en œuvre, à l'application et au développement de l'acquis de Schengen ([273]).

(180) En ce qui concerne la Suisse, la présente décision d'exécution constitue un développement des dispositions de l'acquis de Schengen au sens de l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen ([274]).

(181) En ce qui concerne le Liechtenstein, la présente décision d'exécution constitue un développement des dispositions de l'acquis de Schengen au sens du protocole signé entre l'Union européenne, la Communauté européenne, la Confédération suisse et la Principauté de Liechtenstein sur l'adhésion de la Principauté de Liechtenstein à l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen ([275]),

---

([271]) Avis 15/2021 concernant le projet de décision d'exécution de la Commission européenne conformément à la directive (UE) 2016/680 concernant le niveau de protection adéquat des données à caractère personnel au Royaume-Uni, disponible à l'adresse suivante: https://edpb.europa.eu/our-work-tools/our-documents/opinion-led/opinion-152021-regarding-european-commission-draft_en.

([272]) Décision d'exécution (UE) 2020/1745 du Conseil du 18 novembre 2020 relative à la mise en œuvre des dispositions de l'acquis de Schengen dans le domaine de la protection des données et à la mise en œuvre à titre provisoire de certaines dispositions de l'acquis de Schengen en Irlande (JO L 393 du 23.11.2020, p. 3).

([273]) JO L 176 du 10.7.1999, p. 36.

([274]) JO L 53 du 27.2.2008, p. 52.

([275]) JO L 160 du 18.6.2011, p. 21.

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

Aux fins de l'article 36 de la directive (UE) 2016/680, le Royaume-Uni assure un niveau de protection adéquat des données à caractère personnel transférées de l'Union européenne vers des autorités publiques du Royaume-Uni compétentes pour la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution des sanctions pénales.

Article 2

Lorsque, afin de protéger des personnes à l'égard du traitement de leurs données à caractère personnel, les autorités de contrôle compétentes des États membres exercent leurs pouvoirs en vertu de l'article 47 de la directive (UE) 2016/680 en ce qui concerne les transferts de données vers les autorités publiques au Royaume-Uni dans le cadre du champ d'application de l'article 1er, les États membres concernés en informent la Commission sans délai.

Article 3

1. La Commission surveille de manière continue l'application du cadre juridique sur lequel se fonde la présente décision, notamment les conditions dans lesquelles les transferts ultérieurs sont effectués et les droits individuels exercés, dans le but de déterminer si le Royaume-Uni continue d'assurer un niveau de protection adéquat au sens de l'article 1er.

2. Les États membres et la Commission s'informent mutuellement des cas dans lesquels le commissaire à l'information, ou toute autre autorité compétente du Royaume-Uni, échoue à faire respecter le cadre juridique sur lequel se fonde la présente décision.

3. 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 du Royaume-Uni 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.

4. Lorsqu'elle est en possession d'éléments indiquant qu'un niveau de protection adéquat n'est plus assuré, la Commission en informe les autorités compétentes du Royaume-Uni et peut suspendre, abroger ou modifier la présente décision.

5. La Commission peut suspendre, abroger ou modifier la présente décision si le défaut de coopération de la part du gouvernement du Royaume-Uni l'empêche de déterminer si le constat établi à l'article 1er est affecté.

Article 4

La présente décision vient à échéance le 27 juin 2025, à moins qu'elle ne soit prolongée conformément à la procédure prévue à l'article 58, paragraphe 2, de la directive (UE) 2016/680.

Article 5

Les États membres sont destinataires de la présente décision.

Fait à Bruxelles, le 28 juin 2021.

Par la Commission
Didier REYNDERS
Membre de la Commission