4 Le rôle des données dans le renforcement de la confiance des citoyens

Le présent chapitre explicite tout d'abord les déterminants de la confiance afin de mieux cerner les points clés qui contribuent à donner confiance dans les institutions. Puis il explore le potentiel que recèle l'utilisation des données pour construire la confiance, notamment par l'adoption d'une démarche éthique, la protection de la confidentialité des données, l'instauration de la transparence et l'atténuation des risques. Ce chapitre présente ensuite des exemples de pays qui ont mis en œuvre de bonnes pratiques avec succès, et se conclut par une liste d'orientations déontologiques qui pourraient aider les fonctionnaires à gérer l'utilisation des données d'une manière conforme à l'éthique.

Les données statistiques concernant Israël sont fournies par les autorités israéliennes compétentes et sous leur responsabilité. L'utilisation de ces données par l'OCDE est sans préjudice du statut des hauteurs du Golan, de Jérusalem-Est et des colonies de peuplement israéliennes en Cisjordanie aux termes du droit international.

Introduction

Lorsqu'un pays remplit toutes les conditions d'une bonne gouvernance des données (chapitre 2), il se met en bonne position pour tirer parti des données aux fins d'améliorer les politiques publiques ainsi que la conception et la réalisation des services publics (chapitre 3) et de renforcer ainsi le bien-être des citoyens. Grâce à ce processus, la qualité des services publics répond mieux aux besoins des citoyens. Pourtant, ce processus s'accompagne de la nécessité de renforcer l'accent mis sur les efforts engagés pour renforcer la confiance des citoyens dans l'usage que fait l'administration de leurs données.

Pour nombre d'administrations, élargir l'accès aux données tout en conservant la confiance des administrés relève du défi. Étant donné que la confiance est difficile à gagner et à conserver, et encore plus difficile à restaurer une fois perdue, il est et restera toujours crucial que les administrations s'emploient à préserver la confiance du public. Il est donc important non seulement d'explorer les déterminants de la confiance (réactivité, fiabilité, intégrité, ouverture et équité) et de comprendre comment les règles et les pratiques en matière d'utilisation des données permettent de maintenir la confiance, mais aussi d'examiner comment la confiance peut disparaître si l'utilisation des données n'est pas soigneusement anticipée. Cette démarche permet de mieux appréhender le concept de confiance eu égard à l'utilisation des données dans le secteur public.

Le présent chapitre étudie comment les administrations s'y prennent pour renforcer la confiance en matière de données. Il examine les moyens concrets qu'emploient les administrations et les citoyens pour collaborer sur quatre aspects qui influent sur l'instauration ou la préservation de la confiance : 1) l'éthique ; 2) la confidentialité et le consentement ; 3) la transparence ; et 4) la sécurité.

Ce chapitre est structuré comme suit. Il explicite tout d'abord les déterminants de la confiance afin de mieux cerner les points clés qui contribuent à donner confiance dans les institutions. Puis il explore le potentiel que recèle l'utilisation des données pour construire la confiance, notamment par l'adoption d'une démarche éthique, la protection de la confidentialité des données, l'instauration de la transparence et l'atténuation des risques. Ce chapitre présente ensuite des exemples de pays qui ont mis en œuvre de bonnes pratiques avec succès, et se conclut par une liste d'orientations déontologiques qui pourraient aider les fonctionnaires à gérer l'utilisation des données d'une manière conforme à l'éthique.

Les déterminants de la confiance

Les chercheurs donnent différentes définitions de la confiance (McKnight et Chervany, 2000[1]). Le terme « confiance » sera défini ici comme la conviction d'un individu selon laquelle une autre personne ou une institution adoptera systématiquement le comportement positif auquel il s'attend, d'après le document (OCDE, 2017[2]).

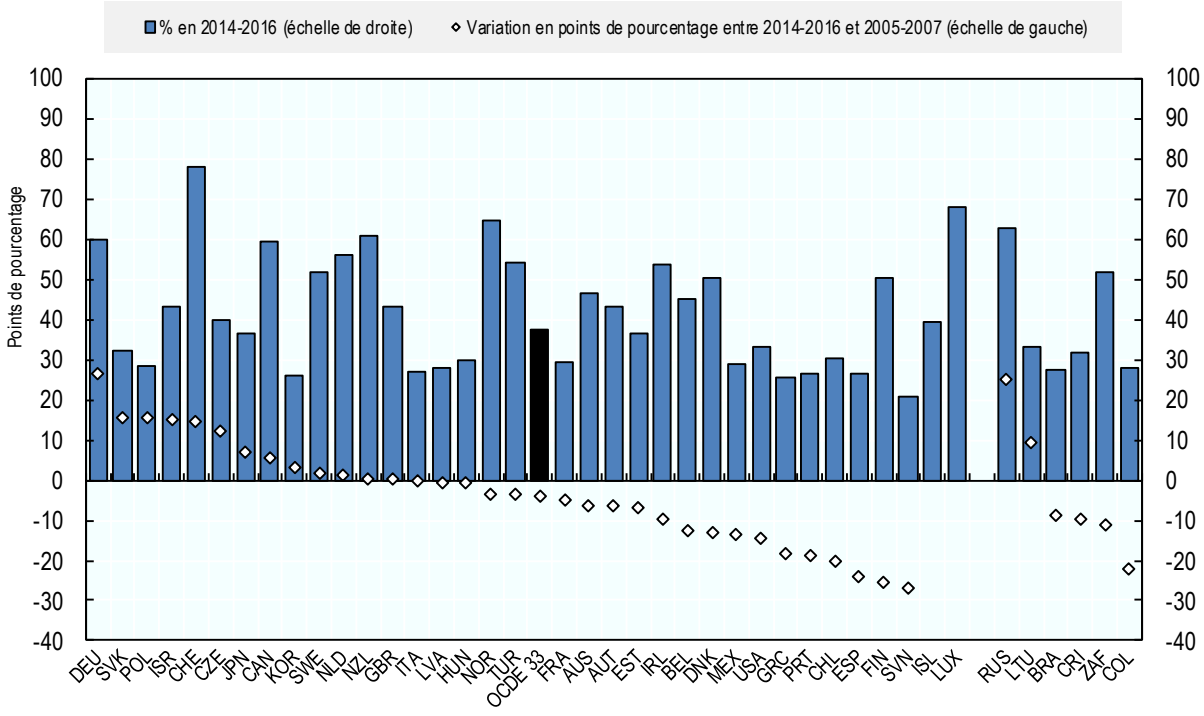
De nombreux chercheurs ont déterminé que la confiance était un facteur majeur de progrès économique et social (Putman, Leonardi et Nanetti, 1993[3] ; Ahn et Hemmings, 2000[4]). La confiance dans une institution aussi bien que la confiance dans une personne ont une incidence sur le revenu par habitant et les progrès économiques d'un pays, sur l'état de santé et les comportements sanitaires, sur le taux de criminalité ainsi que sur le bien-être personnel. Le déclin de la confiance dans les institutions publiques s'explique par de grands événements survenus au cours de la dernière décennie, comme la réaction des pouvoirs publics et l'état de préparation face aux catastrophes naturelles ou à la crise financière de 2008. Cette érosion de la confiance a donné lieu à un essor du populisme et un recul de la participation électorale, dont les niveaux sont alarmants dans de nombreux pays de l'OCDE (Murtin et al., 2018[5]).

Les données montrent que, entre les périodes 2005-2007 et 2014-2016, la confiance des citoyens à l'égard des pouvoirs publics a diminué en moyenne de quatre points dans les pays de l'OCDE (graphique 4.1).

Seuls 38 % des participants ont déclaré avoir confiance dans leur administration nationale (OCDE, 2018[6]).

Pour étudier ce phénomène, l'OCDE a mené des recherches sur les déterminants de la confiance et élaboré un cadre qui examine la confiance sous trois angles différents : individuel, institutionnel et sociétal. Au niveau institutionnel, les citoyens sont invités à collaborer et à avoir confiance dans les institutions elles-mêmes. Les conclusions des enquêtes montrent que les individus, au moment de prendre des décisions et de décider s'ils peuvent faire confiance à une institution, se basent sur le niveau de compétence avec lequel elle remplit sa mission ainsi que sur les valeurs de secteur public qu'elle sert (OCDE/KDI, 2018[7]).

Graphique 4.1. Niveau moyen de confiance dans les administrations nationales sur la période 2014-2016, et variation par rapport à la période 2005-2007



Note : la moyenne de l'OCDE est pondérée en fonction de la population ; l'Islande et le Luxembourg sont exclus parce que les données sont incomplètes.
Source : calculs OCDE d'après l'enquête Gallup World Poll, www.gallup.com/services/170945/world-poll.aspx.

Les compétences des pouvoirs publics se mesurent selon deux dimensions : 1) la réactivité – l'efficacité avec laquelle ils répondent aux besoins et attentes des citoyens tout en évoluant au fil du temps afin de répondre à la demande ; et 2) la fiabilité, c'est-à-dire l'aptitude à réduire et gérer l'incertitude sociale, économique et politique de manière efficace. Les citoyens sont plus enclins à accorder leur confiance à des institutions qui parviennent à fournir des services publics de qualité et adaptés aux bénéficiaires ; les recherches montrent en effet que la confiance dite « institutionnelle » est étroitement liée à la satisfaction à l'égard des services publics (Murtin et al., 2018[5]). Cette corrélation est en particulier plus forte au niveau local qu'au niveau central, car les administrations locales interagissent plus fréquemment avec les citoyens et sont donc plus à même d'offrir de meilleures solutions et de conserver la confiance du public (OCDE, 2017[8]). Cette constatation confirme l'idée que de meilleurs services à la clientèle contribuent à renforcer la confiance (Aberbach, 2007[9]).

Les valeurs de l'administration reposent sur trois piliers : 1) l'intégrité, synonyme d'un faible niveau de corruption au sein du système et d'un degré élevé de redevabilité ; 2) l'ouverture, qui clarifie le processus de participation des citoyens à l'action publique ; et 3) l'équité, c'est-à-dire le traitement homogène et semblable de tous les groupes de citoyens. La confiance de la population à l'égard des institutions est souvent en rapport avec le degré de corruption perçu. Lorsque le niveau de confiance est faible, les institutions rencontrent généralement plus de difficulté à instaurer l'intégrité ; et lorsque la société présente un manque de confiance et de faibles normes de coopération, le non-respect des textes législatifs et réglementaires est plus facilement toléré. De plus, l'expérience de la discrimination influence aussi la perception qu'a la population de l'équité et de la fiabilité des décideurs au sein de l'administration (Murtin et al., 2018[5]).

Une robuste adhésion aux valeurs de l'administration est importante. Plusieurs études internationales ont montré qu'il existait une relation positive entre le niveau de confiance institutionnelle et la qualité du système juridique (c'est-à-dire l'application de la protection des droits de propriété, la redevabilité ou la corruption) (Murtin et al., 2018[5]). En Suisse, par exemple, plus la participation démocratique est forte dans un canton, plus la fraude fiscale est faible. Cela témoigne de l'importance que revêtent l'inclusion et l'engagement démocratiques pour l'émergence de comportements coopératifs.

Tableau 4.1. Cadre des compétences et valeurs sous-tendant la confiance des citoyens dans les institutions publiques : résumé

Composante de la confiance	Mandat de l'administration	Éléments clés	Objectif global de l'action publique
Compétences : aptitude de l'administration à offrir aux citoyens les services dont ils ont besoin, au niveau de qualité qu'ils attendent	Fournir des services publics	Accès de tous aux services publics, indépendamment des conditions socioéconomiques Qualité et rapidité de la prestation des services publics Respect montré dans la fourniture des services publics, notamment réponses apportées aux réactions des citoyens	Réactivité
	Anticiper le changement, protéger les citoyens	Anticipation et évaluation adéquate de l'évolution des besoins des citoyens et des défis à relever Comportement constant et prévisible Gestion efficace des incertitudes sociales, économiques et politiques	Fiabilité
Valeurs : déterminants et principes qui informent et guident l'action publique	Utiliser le pouvoir et les ressources publiques de manière éthique	Normes de comportement rigoureuses Engagement de lutte contre la corruption Redevabilité	Intégrité
	Informer, consulter et écouter les citoyens	Aptitude à connaître et comprendre l'action de l'administration Opportunités de participation qui conduisent à des résultats tangibles	Ouverture
	Améliorer les conditions socioéconomiques pour tous	Poursuite des progrès socioéconomiques dans l'ensemble de la société Traitement homogène des citoyens et des entreprises (cf. craintes de détournement)	Équité

Source : OCDE (2017[8]), Trust and Public Policy: How Better Governance Can Help Rebuild Public Trust, http://dx.doi.org/10.1787/9789264268920-en.

D'après le tableau 4.1, la réactivité, la fiabilité, l'intégrité, l'ouverture et l'équité sont les cinq déterminants de la confiance institutionnelle qui peuvent aider l'administration à restaurer, préserver ou relever le degré de confiance du public. Cependant, pour que les pouvoirs publics puissent répondre à ces cinq exigences, ils doivent se concentrer sur la fourniture de services publics qui satisfont aux besoins des citoyens

(chapitre 3). C'est pourquoi une démarche axée sur les données, assortie d'une participation des citoyens, de l'ouverture de l'administration et d'une collaboration de toutes les parties prenantes, est une nécessité.

De fait, les pouvoirs publics utilisent des données pour informer les responsables publics quant aux processus de prise de décision et pour créer de la valeur publique. Nombre d'organisations publiques et privées font appel aux données en tant que ressources, non seulement pour améliorer des produits et services existants, mais aussi pour en créer de plus innovants, recueillir des retours d'information et, surtout, comprendre les besoins des usagers. Dans cette optique, les technologies numériques ne doivent plus être utilisées comme un simple outil permettant d'offrir une valeur publique qui serait déterminée par ces technologies, et en particulier par les données, ce qui s'accompagne aussi d'une exigence de bonne gouvernance des données (OCDE, 2019[10]).

Une bonne gouvernance des données, comme le montre le chapitre 2, a le pouvoir de relever la qualité des services publics. En améliorant l'accessibilité et la disponibilité des données, elle permet aux administrations de fournir des services qui sont plus réactifs, fiables, éthiques, ouverts et équitables. En dépit de leurs effets positifs sur l'amélioration du bien-être des citoyens, l'utilisation, l'analyse et la collecte de données à grande échelle posent des problèmes éthiques pressants, parfois nouveaux. Ainsi, le fait que les données ne se prêtent pas à la rivalité, c'est-à-dire qu'elles peuvent être reproduites et utilisées simultanément par plusieurs personnes et à des fins autres que le but dans lequel elles ont été recueillies, accentue la complexité de ces problèmes et exige des limites strictes.

L'éthique en matière de données, socle de la confiance du public

En ce XXIe siècle, les données offrent de multiples possibilités d'améliorer l'action publique, ainsi que la conception et la prestation des services publics, et contribuent ainsi au bien-être des citoyens. Néanmoins, les opportunités s'accompagnent souvent de difficultés. L'usage croissant des données – personnelles aussi bien que non personnelles –, leur disponibilité et leur accessibilité soulèvent un grand nombre de questions, non seulement quant au caractère éthique de leur utilisation, de leur collecte, de leur traitement et de leur stockage, mais aussi au sujet des dimensions de responsabilité, de redevabilité, d'équité et de respect des droits humains figurant dans la législation actuelle en matière de données.

L'attitude des citoyens à l'égard des pratiques de l'administration en matière de données évolue rapidement, et l'intérêt pour une approche éthique de la gestion des données ne cesse de croître. Les atteintes très médiatisées à la protection des données, l'influence des géants des technologies (BigTech) dans le secteur privé et l'élaboration de règlements à ce sujet ont sensibilisé le grand public aux modalités de traitement des données. Les citoyens sont de plus en plus préoccupés par la manière dont les pouvoirs publics abordent ce domaine. Le traitement réservé aux données au sein d'une organisation dépend de la vision que celle-ci a des données, laquelle dépend à son tour, entre autres, de ses dirigeants (chapitre 2) et de sa culture globale. La direction doit veiller à instaurer une culture des données responsable. Il est essentiel qu'une administration ait des valeurs et une culture d'utilisation responsable des données pour que celles-ci puissent être recueillies, stockées et analysées de manière éthique et transparente.

Montrer que les pouvoirs publics apportent leur attention à chaque stade du cycle de valeur des données publiques (graphique 3.1 au chapitre 3) est une étape clé dans le renforcement de la confiance. L'érosion de la confiance dans l'administration ralentit la mise en œuvre des politiques publiques. Par conséquent, il est essentiel de déployer des efforts visant à mettre en place une solide culture d'utilisation éthique des données afin d'instaurer des conditions propres à optimiser l'impact des pratiques axées sur les données au sein du secteur public.

L'éthique des données est une branche de l'éthique qui s'intéresse à ces questions en relation avec la confiance du public. Les chercheurs définissent comme suit l'éthique en matière de données : il s'agit d'une nouvelle branche de l'éthique qui étudie et évalue les problèmes liés aux données (production,

enregistrement, conservation, traitement, diffusion, partage et utilisation), aux algorithmes (intelligence artificielle, agents artificiels, apprentissage machine et robots) et aux pratiques correspondantes (innovation responsable, programmation, piratage informatique et codes professionnels), afin de formuler et d'encourager des solutions moralement bonnes (bonnes conduites ou bonnes valeurs) (Floridi et Taddeo, 2016[11]).

L'accent mis sur l'éthique des données est de plus en plus marqué, non seulement parce que l'approche auparavant centrée sur l'information est désormais axée sur les données (Floridi et Taddeo, 2016[11]), mais aussi parce que les organisations sont invitées à établir leur propre jeu de principes et de processus en matière de données. Au cours des 30 dernières années, l'attention s'est portée sur les problèmes éthiques découlant de l'usage des ordinateurs et des technologies numériques. Des outils technologiques spécifiques comme les ordinateurs, les tablettes, l'informatique en nuage, etc., étaient au centre de ces stratégies éthiques, alors que, aujourd'hui, l'éthique des données porte sur la manière dont la technologie est utilisée, ce qui a affiné l'approche et contribué à l'évolution de l'éthique des ordinateurs et de l'information (Floridi et Taddeo, 2016[11]). Ainsi, c'est la ressource utilisée, les données en l'occurrence, qui doit être la priorité, et non la technologie qui permet de la traiter. L'usage des données est facilité lorsqu'il est encadré par des limites, afin d'en tirer le meilleur parti au bénéfice de la société.

Différents secteurs de l'action publique et organisations sont encouragés à élaborer leurs propres principes en matière de données afin de rendre leurs pratiques plus éthiques et transparentes et, partant, plus dignes de confiance. De fait, pour conserver la confiance des citoyens, il est fondamental de mettre en place des pratiques claires au sujet des données. Un traitement correct des données peut permettre de trouver le juste équilibre entre innovation et pratiques éthiques eu égard aux données, tout en plaçant l'usager au centre du processus de conception des produits et services. Pour que cela puisse se produire, les citoyens doivent comprendre comment les données qui les concernent sont collectées, analysées et conservées, et pendant combien de temps, afin qu'ils puissent constater la valeur créée à partir de leur apport, ainsi que les valeurs et la culture de l'administration qui traite ces données. Par conséquent, donner aux citoyens les moyens de comprendre la confiance publique et de s'y associer est une démarche fondamentale, car la voix et l'autonomie des citoyens constituent des composantes importantes dans le renforcement de la confiance, tout en favorisant l'inclusion numérique (encadré 4.1). On est ainsi ramené au concept de cycle de valeur des données publiques (van Ooijen, Ubaldi et Welby, 2019[12]), qui montre comment les différentes étapes que traversent les données peuvent toutes contribuer à en optimiser la valeur publique (chapitre 3).

Encadré 4.1. L'Appel de Christchurch pour éliminer le terrorisme et l'extrémisme violent en ligne

En réponse à l'attentat terroriste du 15 mars 2019 survenu à Christchurch, en Nouvelle-Zélande, Jacinda Ardern, Première Ministre de Nouvelle-Zélande, et Emmanuel Macron, Président de la République française, ont lancé une initiative inédite, associant le grand public, et ont réuni à Paris des chefs d'État et de gouvernement ainsi que des dirigeants d'entreprises du numérique pour les inviter à signer l'Appel de Christchurch.

L'Appel de Christchurch engage les pouvoirs publics et les entreprises du secteur de la technologie à éliminer les contenus terroristes et extrémistes en ligne. Il repose sur une conviction : un internet ouvert, libre et sûr, nous offre des bénéfices extraordinaires.

Comme l'attentat a été diffusé en direct sur internet, est devenu viral et a persisté sur le web malgré les mesures prises pour supprimer la vidéo, il est important que la population ait conscience que la diffusion de ce type de contenu sur internet a des effets délétères sur les droits des victimes, sur notre sécurité collective et sur les populations du monde entier.

Des mesures importantes ont déjà été prises pour lutter contre ce danger, que ce soit, entre autres, par la Commission européenne à travers d'initiatives telles que le Forum de l'Union européenne sur l'internet, par le G20 et le G7, y compris dans le cadre des travaux en cours menés sous la présidence française du G7 dans le domaine de la lutte contre l'utilisation de l'internet à des fins de terrorisme et d'extrémisme violent, ainsi que par le Forum mondial de l'internet contre le terrorisme, le Forum mondial de lutte contre le terrorisme, l'initiative Tech Against Terrorism et le processus d'Aqaba mis en place par le Royaume hachémite de Jordanie.

Les événements de Christchurch ont démontré une nouvelle fois qu'il était urgent d'agir et de renforcer la coopération entre les nombreux acteurs ayant une influence dans ce domaine, notamment les pouvoirs publics, la société civile et les fournisseurs de services en ligne, comme les entreprises de réseaux sociaux, afin d'éliminer les contenus terroristes et extrémistes violents en ligne.

Cet Appel souligne que toutes les mesures prises pour faire face à ce problème doivent être conformes aux principes d'un internet libre, ouvert et sûr, dans le respect des droits humains et des libertés fondamentales, y compris la liberté d'expression. Elles doivent également tenir compte du fait que l'internet peut avoir une action bénéfique, notamment à travers la promotion de l'innovation et du développement économique, mais aussi en favorisant l'intégration sociale, ce qui contribue à préserver la confiance des citoyens dans leurs autorités nationales.

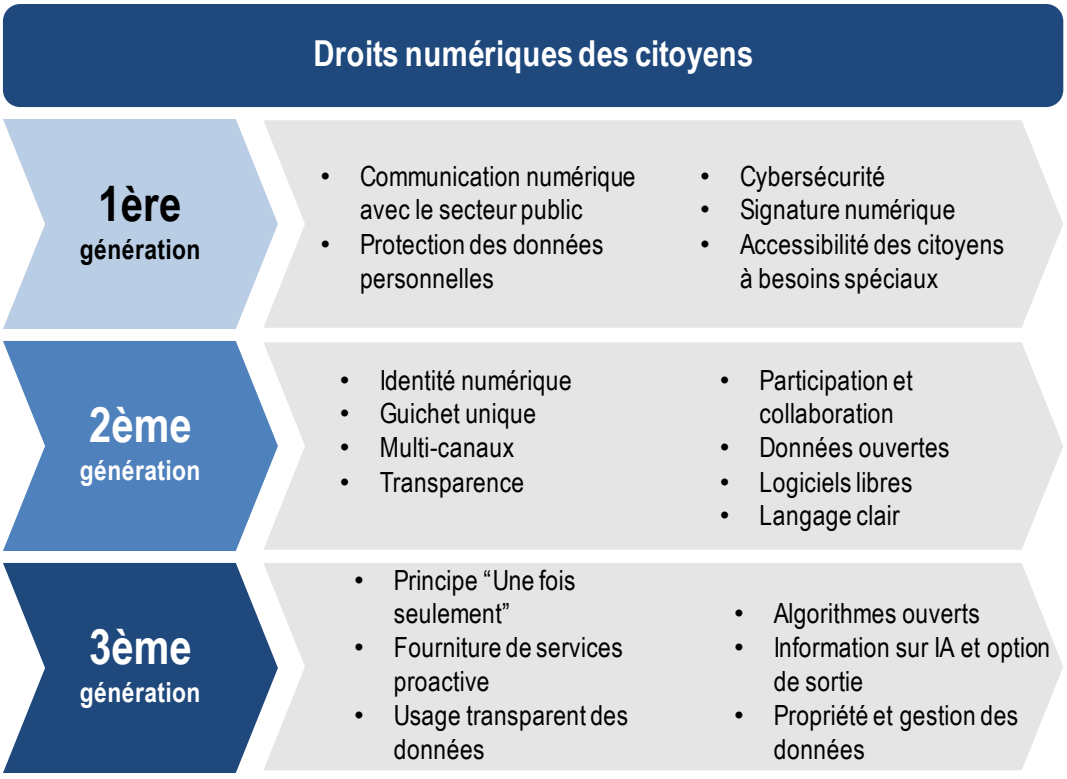
Source : Ministère néo-zélandais des Affaires étrangères et du Commerce (2019[13]), Appel de Christchurch, https://www.appeldechristchurch.com/appel.html.

Droits numériques et droits en matière de données

Les administrations publiques s'orientent progressivement vers une transformation participative rendue possible par l'utilisation plus poussée des données personnelles aux fins d'offrir des services publics de qualité. Elles ont donc la responsabilité de garantir la protection des droits numériques des citoyens. À cette fin, les administrations intensifient les efforts juridiques et réglementaires qu'elles déploient pour remédier aux nouveaux problèmes qui émergent à ce sujet en cette ère numérique. Inspiré par l'évolution des droits humains, le graphique 4.2 est une ébauche de classement des droits numériques en trois générations. Ces catégories ne sont pas clairement délimitées, mais permettent simplement d'établir des distinctions ; de même, la plupart des droits peuvent se classer dans plus d'une catégorie, ce qui laisse ce projet de cadre ouvert au débat.

À l'instar des droits humains de première génération (droits civiques et politiques), les droits numériques de première génération devraient de fait être considérés comme des droits fondamentaux des citoyens : protection des données personnelles, droit à la communication numérique avec le secteur public et cybersécurité (OCDE, 2019[13]) (graphique 4.2).

Graphique 4.2. Droits numériques : vers une transformation participative



Source : OCDE (2019[13]), *Digital Government Review of Panama: Enhancing the Digital Transformation of the Public Sector*, https://doi.org/10.1787/615a4180-en.

Par exemple, la Constitution mexicaine a, dès 2013, intégré l'accès à internet parmi les droits humains et garanti une stricte impartialité (Freedom House, 2018[14]). Un autre exemple est celui de la stratégie pour un marché unique numérique, proposée par la Commission européenne en 2015, au titre de laquelle 17 propositions législatives ont été acceptées, et 12 autres sont en cours d'examen (Commission européenne, 2019[15]). Les citoyens européens jouissent, depuis 2016, du droit d'accéder librement à l'internet, sans discrimination quant à leur choix de contenu et, depuis 2018, d'accéder gratuitement à leur abonnement télévision, sports et musique lorsqu'ils sont en voyage au sein de l'UE.

Cependant, compte tenu du développement des technologies, y compris la diffusion rapide d'un pays à l'autre de technologies émergentes comme l'intelligence artificielle, il devient essentiel que les États protègent les droits numériques de deuxième génération (droits humains économiques et sociaux), voire de troisième génération (droits humains collectifs au développement) (OCDE, 2019[13]), en revenant sur la compréhension existante des droits numériques et des mesures juridiques qui s'y appliquent. En moyenne, la plupart des pays de l'OCDE couvrent les droits numériques de deuxième génération. Au Panama, par exemple, l'État a mis moins d'une décennie à adopter une approche axée sur les droits numériques. De nombreuses lois ont été adoptées, comme celle qui protège le droit des citoyens à une interaction numérique avec le secteur public (Asamblea Nacional, 2012[16]), l'application du principe « une fois seulement », la politique nationale sur les données publiques ouvertes (Asamblea Nacional, 2012[16]) (Ministerio de la Presidencia, 2017[17]) ainsi qu'une réglementation relative aux données personnelles

(Asamblea Nacional, 2019[18]). Des exemples concernant d'autres pays sont donnés plus loin dans ce chapitre.

L'adoption du règlement général sur la protection des données (RGPD), en 2018, produit ses effets dans toute l'Union européenne. Élaboré dans le but de protéger la confidentialité et les données personnelles des citoyens européens, ce règlement a entraîné une modification des lois existantes ainsi que l'adoption de nouvelles lois. Au Portugal, cela s'est traduit par une initiative prioritaire à haut niveau, destinée à examiner toute nouvelle réglementation ou adaptation requise pour répondre à ces questions, qui sont dévolues aux États membres.

Reconnaître les droits numériques et trouver des moyens de les protéger est une démarche nécessaire mais non suffisante pour créer un environnement sûr et susciter la confiance mutuelle. Les dispositions légales et réglementaires doivent aller de pair avec des principes moins contraignants, comme des orientations, qui seront adoptées par les administrations et largement utilisées dans le secteur public. Face à cette nécessité, les pays ont adopté des mesures spécifiques sur les droits relatifs aux données ainsi que des textes de lois, qui sont examinés dans la prochaine section. De plus, l'OCDE procède actuellement, en collaboration avec ses pays Membres, à l'élaboration de lignes directrices pour l'éthique en matière de données, qui sont également étudiées plus loin dans ce chapitre. Afin de nourrir la confiance, les pratiques réglementaires et les principes doivent couvrir les quatre domaines essentiels : éthique, confidentialité et consentement, transparence et sécurité.

Textes relatifs à la bonne gouvernance des données dans les pays de l'OCDE

De nombreux pays semblent accorder une haute priorité à ces quatre piliers que sont l'éthique, la confidentialité et le consentement, la transparence et la sécurité, et les abordent suivant une approche légaliste. Bien que le rôle des autorités soit de protéger les données des citoyens et de veiller au respect des droits fondamentaux et de la liberté des citoyens dont les données sont utilisées, les pouvoirs publics établissent aussi leurs priorités en fonction des besoins des citoyens et des problèmes auxquels ils sont confrontés. À cette fin, de nombreux efforts réglementaires ont été déployés pour rendre ce processus transparent et accessible.

En **Corée**, par exemple, la Commission de protection des informations personnelles est légalement tenue d'établir, tous les trois ans, un plan directeur destiné à assurer la protection des informations personnelles ainsi que des droits et intérêts des personnes concernées. De plus, les responsables des organes administratifs centraux doivent établir et réaliser chaque année un plan d'exécution pour la protection des données personnelles aux termes de ce plan directeur. Sur une base permanente, tout changement apporté aux politiques, systèmes ou statuts s'accompagne obligatoirement d'une évaluation des risques de violation de la protection des données, qui est ensuite rendue publique (Gouvernement de la Corée, 2019[19]). Cette démarche montre que la confidentialité et la transparence étaient des questions sur lesquelles la Corée devait rapidement se pencher.

Le **Royaume-Uni**, qui a promptement réagi à l'évolution technologique, fait en sorte que sa législation (par exemple, la loi sur l'économie numérique et la loi sur la protection des données) ne soit pas en retard sur l'innovation, afin d'assurer la protection des données personnelles et de la vie privée des citoyens. Ainsi, le programme numérique du Royaume-Uni tempère constamment le potentiel des nouvelles formes de technologie en faisant preuve de prudence quant à l'utilisation des données personnelles. Il fait appel tant à des spécialistes externes, issus de la société civile, qu'à différentes équipes au niveau ministériel pour s'assurer que les travaux sur les données sont attentivement étudiés et que les régimes de protection et de confidentialité des données sont strictement appliqués.

Le **Portugal** a choisi de faire de la sécurité le principe directeur prioritaire de sa Stratégie TIC 2020, placée sous le signe des données – leur sécurité, leur résilience et leur confidentialité. Le pays a pris des initiatives

pour réduire les risques associés à la sécurité numérique. La Commission nationale pour la protection des données est chargée de s'assurer que la législation sur la protection des données est bien appliquée, et que, de ce fait, la sécurité numérique est effectivement prise en compte. Ce travail vient compléter celui du Cabinet national pour la sécurité du Portugal, qui assure la sécurité des informations classées confidentielles et auquel il revient d'autoriser les particuliers et les entreprises à accéder à ces informations et à les utiliser. De plus, le Centre national pour la cybersécurité veille à ce que le Portugal utilise l'internet de manière libre, fiable et sûre.

Bien que les pouvoirs publics appliquent différentes méthodes pour remédier aux problèmes de confiance dans leur pays, il se dégage, dans leurs opérations et activités, une certaine cohérence dans les efforts portant sur quatre domaines. Ces quatre axes de travail se sont dégagés à partir des recherches, des examens et des rapports sur l'administration numérique (Welby, 2019[20] ; van Ooijen, Ubaldi et Welby, 2019[12] ; OCDE, à paraître[21]), qui laissent penser que la confiance se construit et se maintient en s'appuyant sur les piliers suivants :

- respect de l'éthique : une démarche éthique guidant les comportements dans l'ensemble du secteur public ;
- confidentialité : protection de la vie privée des citoyens et établissement des droits aux données ;
- transparence : transparence des algorithmes utilisés pour la prise de décision publique et reddition de comptes à ce sujet ;
- sécurité : gestion des risques qui pèsent sur les données publiques.

Respect de l'éthique

Un traitement des données conforme à l'éthique ne nuit à personne, directement ou indirectement, et ce, même si la diffusion des données est légale. Il s'agit d'un aspect de grande envergure, puisqu'il couvre toutes les dimensions du cadre, dont une facette cruciale réside dans le fait qu'une pratique non conforme à l'éthique n'est pas nécessairement illégale. Par exemple, publier les données personnelles relatives à des services d'interruption de grossesse, comme le nom, la clinique et la date, dans un endroit où cet acte est jugé inacceptable et où les femmes sont susceptibles d'être victimes de violence, serait une pratique non éthique, même si la publication de ces informations est autorisée par la loi (ODI, 2017[22]). Ainsi, il est essentiel que les pouvoirs publics prennent l'initiative sur le plan de l'éthique, pour guider la prise de décision et informer les comportements en matière de données.

Plusieurs pays s'imposent l'obligation officielle de formuler leurs principes de collecte, de traitement, de partage, d'accessibilité et de réutilisation des données afin de prévenir, et de sanctionner, tout comportement qui serait contraire à l'intérêt public. La législation est l'une des voies possibles pour assurer une gestion et une utilisation éthiques des informations personnelles, tant dans le secteur public que privé. Dans cette optique, la Corée a créé un Portail pour la protection des données personnelles (Korean Ministry of the Interior and Safety, 2019[23]), afin de sensibiliser le grand public à cette question ; ce portail propose notamment des modules d'éducation en ligne, offrant des programmes sur mesure pour les particuliers et les entreprises qui souhaitent améliorer leur connaissance de la gestion et de l'utilisation éthiques des données. Aux fins de cette initiative, dix principes ont été élaborés à l'intention des citoyens et des entreprises, pour prévenir toute violation de la confidentialité d'informations personnelles. En ce qui concerne les entreprises, des évaluations sont menées pour déterminer si elles respectent les obligations et les principes de la protection des données personnelles, la dépersonnalisation des informations privées, la fourniture d'une assistance technique et la gestion des données d'identification (Korean Ministry of Public Administration and Security, 2019[24]).

Il est toutefois important de noter que, de plus en plus, la mise sur pied de cadres éthiques est un moyen d'éviter l'adoption d'une réglementation. Comme l'éthique est souvent considérée comme une option

« simple » ou « douce » pour l'autorégulation des pratiques numériques, de nombreuses organisations privées y font appel pour leurs procédures de prise de décision, par exemple dans le cas suivant :

> *Lors de la Conférence sur les affaires mondiales de 2018, l'une des participantes à l'équipe d'éthique de Google DeepMind, membre d'un panel sur l'éthique, a souligné à de nombreuses reprises que Google DeepMind opérait en totale conformité avec l'éthique, en refusant cependant toute responsabilité dans le scandale sur la protection des données qui avait éclaté à Google DeepMind (Powles et Hal, 2018[25]). D'après elle, Google DeepMind était une société conforme à l'éthique, élaborant des produits éthiques, et le fait que les données de santé de 1.6 million de personnes soient mises en partage hors de toute base légale relevait plutôt de la responsabilité des autorités britanniques. (Wagner, 2018[26])*

B. Wagner affirme qu'il est fondamental de disposer de critères à l'aune desquels mesurer le respect de l'éthique. Dans le cas où ces critères communs ne sont pas respectés, le risque est que nombre de cadres d'éthique deviennent arbitraires, optionnels ou dénués de sens, alors qu'ils devraient être substantiels, effectifs et rigoureux (Wagner, 2018[26]).

Pour veiller au respect des pratiques éthiques, les pays ont mis sur pied des organes indépendants et élaboré des cadres régissant la gestion et l'utilisation des données. Les pratiques nationales présentées ci-dessous illustrent les différents moyens de créer un environnement éthique.

Le respect de l'éthique contrôlé par une entité indépendante

Les pouvoirs publics peuvent promouvoir un comportement éthique en s'appuyant sur un organisme principal chargé des données détenues par l'administration. Son rôle consiste à aider les organismes publics à renforcer leurs capacités et à gérer les données qu'ils détiennent sur les citoyens comme un précieux actif stratégique, à faciliter l'accès aux données, à appliquer des normes en matière de données et à tester de nouvelles méthodes. Ainsi, l'**Irlande** et le **Portugal** ont créé des organisations spéciales chargées de s'approprier ce programme.

En **Irlande**, il s'agit du Bureau du Commissaire à la protection des données (Data Protection Commission, 2019[27]) ; au **Portugal**, la Commission nationale pour la protection des données (CNDP) est une entité indépendante dotée de pouvoirs couvrant l'ensemble du pays. Cette commission supervise et surveille la conformité avec les lois et règlements en matière de protection des données personnelles, le strict respect des droits humains ainsi que des libertés fondamentales et garanties inscrites dans la Constitution et dans la loi. Par exemple, les entités publiques et privées doivent notifier le CNPD au sujet de tout traitement de données personnelles qu'ils effectuent.

Cette méthode de mise en œuvre d'un comportement éthique est particulièrement commune dans les pays abritant des peuples autochtones. Comme les données relatives aux peuples autochtones constituent un terrain juridique et éthique d'une grande complexité (Australian National Data Service, 2019[28]), qui doit être géré avec soin, c'est une agence principale chargée des données détenues par l'État qui s'assure que les données sont effectivement traitées de manière conforme à l'éthique. Le Centre de gouvernance de l'information des Premières nations de l'Alberta offre un bon exemple de cette méthode. Un satellite régional du Centre national au **Canada** a été créé par les Premières Nations pour répondre aux besoins du Centre de gouvernance de l'information des Premières nations de l'Alberta. Premier modèle autochtone de recherche, il vise à faciliter l'exercice de la juridiction des Premières Nations et à conférer l'appropriation, le contrôle, l'accès et la possession des données et des informations relatives aux Premières Nations. Ce modèle tient prioritairement compte d'indicateurs culturellement pertinents ; il s'est en effet avéré que certains indicateurs étaient dénués de toute pertinence, soit aux fins de l'interprétation des données eu égard aux communautés concernées, soit pour éclairer les politiques publiques (Healy, 2012[29]).

Le fait de disposer d'une entité indépendante permet aussi de tester des idées, de définir des stratégies et de mesurer les risques. En **Nouvelle-Zélande**, le Commissaire aux services de l'État a décidé, en 2017, que le directeur général de Stats NZ serait l'intendant principal des données publiques. En tant que tel,

son rôle consiste à fixer l'orientation stratégique de la gestion des données publiques. Pour ce faire, il aide les organismes publics à développer leurs capacités et à prendre conscience de la valeur des données qu'ils détiennent en tant qu'actifs stratégiques (encadré 4.2).

Encadré 4.2. Nouvelle-Zélande : le Groupe consultatif sur le traitement éthique des données

Afin que le développement de l'accès aux données et de leur utilisation s'accompagne d'un niveau approprié d'atténuation des risques et de précautions, l'intendant principal des données publiques de Nouvelle-Zélande a fondé le Groupe consultatif sur le traitement éthique des données, dont la vocation première est d'aider les autorités à mieux comprendre les questions relatives aux usages nouveaux et émergents des données, et à formuler des avis et des commentaires à ce sujet.

Pour permettre à ce groupe d'accomplir sa mission, l'intendant principal des données publiques a nommé en tant que membres sept experts indépendants, issus de différents domaines pertinents à l'égard de l'utilisation des données et de l'éthique, notamment le respect de la vie privée et les droits humains, les technologies et l'innovation. L'un des sièges de membre est réservé à un membre du Groupe de co-conception Te Ao Maoru, afin d'appuyer les travaux menés par les Maori sur la gouvernance des données et d'apporter différents points de vue dans le cadre de gouvernance des données de la Nouvelle-Zélande.

Le groupe est seulement habilité à examiner et formuler des commentaires relatifs aux sujets et initiatives en matière d'utilisation des données, sans aborder les solutions numériques plus générales mises en œuvre par les organismes publics. Parmi les exemples de thèmes que le Groupe consultatif sur le traitement éthique des données pourrait être invité à commenter figurent l'usage approprié des algorithmes de données (et comment éviter les biais algorithmiques, notamment) et la bonne mise en œuvre des initiatives en matière de gouvernance des données.

Source : Stats NZ (2019[31]), Data Ethics Advisory Group, https://www.data.govt.nz/about/government-chief-data-steward-gcds/data-ethics-advisory-group (consulté le 27 août 2019).

Le respect de l'éthique encouragé par un cadre ou des orientations

Une autre manière d'instaurer des comportements éthiques consiste, pour les pouvoirs publics, à créer un cadre ou des orientations qui offrent aux usagers des informations, des ressources et des méthodes leur permettant d'adopter des pratiques et des modes de prise de décision conformes à l'éthique. Ce cadre et ces orientations n'ont pas vocation à être contraignants : ils visent à favoriser une appréhension commune de la question et la résolution des questions d'ordre éthique.

Au **Royaume-Uni**, les codes de bonnes pratiques pour l'application des dispositions de partage de données contenues dans la loi sur l'économie numérique prévoient un équilibre des pouvoirs, conformément à la loi sur la protection des données, destiné à éviter toute utilisation frauduleuse et tout partage abusif des données (Ministère britannique du Numérique, 2019[30]). Pour les travaux sur les données qui sortent du champ de la législation, les autorités ont construit un Cadre pour l'éthique des données, dont le développement se poursuit, qui a pour but de guider les décideurs et les analystes de données eu égard aux conséquences éthiques des travaux qu'ils mènent (encadré 4.3).

La **Nouvelle-Zélande** offre un autre exemple de cette méthode. L'intendant principal des données publiques et le Commissaire à la confidentialité des données ont élaboré ensemble six principes clés à l'appui d'une analytique des données sûre et efficace, dont le Cadre pour la confidentialité, les droits humains et l'éthique. Instauré par le ministère du Développement social, ce cadre est un ensemble de capacités et d'outils avec lesquels les utilisateurs d'informations interagissent afin que ces trois principes

fondamentaux soient pris en considération dès le stade de la conception d'une nouvelle initiative (encadré 4.3).

Encadré 4.3. Royaume-Uni : un Cadre pour l'éthique en matière de données

En 2018, le Royaume-Uni a créé un Cadre pour l'éthique en matière de données, destiné à guider les fonctionnaires vers un usage approprié des données. Les fonctionnaires doivent évaluer chaque projet, service ou logiciel acheté en regard des sept principes éthiques ci-dessous, qui sont conçus pour être régulièrement rappelés.

1. Commencez par clarifier les besoins de l'utilisateur et l'avantage pour la population. L'utilisation plus innovante des données recèle un potentiel de transformation de la manière dont les services publics sont assurés. Nous devons toujours définir clairement ce que nous tentons de réaliser pour les usagers – les citoyens comme les fonctionnaires.
2. Informez-vous sur la législation et les codes de bonnes pratiques pertinents. Vous devez avoir compris les lois et codes de bonnes pratiques qui se rapportent à l'utilisation des données. En cas de doute, consultez les spécialistes de ce domaine.
3. Utilisez des données proportionnées aux besoins de l'usager. L'utilisation des données doit être proportionnelle aux besoins de l'usager, c'est-à-dire que vous devez utiliser le minimum de données nécessaires pour atteindre le résultat souhaité.
4. Appréhendez les limitations des données. Les données utilisées pour éclairer la conception des politiques et des services publics doivent être bien comprises. Il est essentiel d'étudier les limites des données lorsqu'on détermine s'il est approprié de les utiliser pour répondre aux besoins d'un usager.
5. Appliquez de saines pratiques et travaillez dans votre champ de compétences. Les apports des nouvelles technologies ne sont valables que s'ils ont été créés sur la base de bonnes données et pratiques. Travaillez dans votre domaine de compétences, et sachez reconnaître les limites de vos compétences ou expérience lorsqu'il s'agit d'utiliser une méthode ou un outil particulier à haut niveau.
6. Veillez à la transparence dans votre travail et prenez soin d'en rendre compte. La transparence s'impose quant aux outils, aux données et aux algorithmes que vous utilisez pour mener à bien votre travail, en travaillant au grand jour lorsque c'est possible. Cela permet à d'autres chercheurs d'étudier vos conclusions et aux citoyens de comprendre les nouveaux types de travaux que vous menez.
7. Inscrivez l'utilisation des données dans un cadre responsable. Il est essentiel de disposer d'un plan permettant de s'assurer que les informations tirées des données font l'objet d'un usage responsable. Cela suppose que les équipes de développement et de mise en œuvre comprennent bien l'usage qu'elles peuvent faire des conclusions et des modèles de données, et mettent en place un solide plan d'évaluation pour en assurer le suivi.

Source : Ministère britannique du Numérique, de la Culture, des Médias et des Sports, (2018[33]), Guidance Data Ethics Framework, https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework#the-data-ethics-framework-principles.

L'usage croissant des technologies émergentes par les administrations aux fins d'améliorer les services publics et les programmes officiels, s'il s'accompagne de l'obligation de veiller au comportement éthique des fonctionnaires dans le traitement des données des citoyens, donne lieu également à un autre ensemble de comportements éthiques. Compte tenu de la complexité des systèmes d'intelligence artificielle (IA), il est crucial de s'assurer que l'IA fait l'objet d'un usage efficace et conforme à l'éthique. Le gouvernement fédéral du **Canada** a exploré l'utilisation responsable de l'IA dans l'administration ; dans ce contexte, il a créé un outil d'évaluation de l'impact algorithmique (EIA), destiné à aider les concepteurs à

évaluer la viabilité de leurs solutions d'IA, et il a mis au point, en complément, un ensemble de principes directeurs (encadré 4.4). L'EIA est un questionnaire conçu pour aider les entreprises et les administrations à évaluer et à atténuer les risques associés au déploiement d'un système automatisé de prise de décision. Il permet aussi de déterminer le niveau d'incidence d'un système automatisé de prise de décision aux termes de la Directive sur la prise de décision automatisée. Les questions portent sur les processus métier, les données et les décisions de conception de système (Gouvernement du Canada, 2019[31]).

Encadré 4.4. Canada : principes directeurs complétant l'Évaluation d'impact algorithmique

Même si les technologies émergentes sont très souvent utilisées pour aider les administrations publiques à prendre des décisions plus éclairées, ceux-ci doivent s'assurer que ces technologies sont utilisées de manière appropriée, dans l'intérêt des citoyens. C'est pourquoi le gouvernement canadien a mis en place une série de principes directeurs visant à garantir une utilisation efficace et éthique de l'IA, venant compléter l'outil d'évaluation de l'impact algorithmique (EIA).

Au sein de l'administration canadienne, tous les fonctionnaires doivent appliquer les règles ci-dessous à l'utilisation de l'IA :

1. comprendre et mesurer l'incidence de l'utilisation de l'IA en concevant et en diffusant des outils et des approches ;
2. faire preuve de transparence quant à la façon et au moment d'utiliser l'IA, en se fondant sur un besoin clair des utilisateurs et l'intérêt du public ;
3. fournir des explications claires sur le processus décisionnel en matière d'IA tout en offrant des occasions d'examiner les résultats et de remettre en question les décisions ;
4. être le plus ouvert possible en communiquant le code source, les données sur la formation et d'autres renseignements pertinents et ce, en protégeant les renseignements personnels, l'intégrité du système, ainsi que la sécurité et la défense nationales ;
5. offrir une formation adéquate pour que les agents publics qui conçoivent et utilisent des solutions liées à l'IA aient les compétences nécessaires en matière de conception, de fonctionnement et de mise en œuvre responsables pour améliorer les services publics fondés sur l'IA.

Source : Gouvernement du Canada (2019[36]), Utilisation responsable de l'intelligence artificielle (IA), https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/technologiques-modernes-nouveaux/utilisation-responsable-ai.html.

Ces exemples nationaux montre que l'instauration d'un environnement éthique est fondamentale pour que de nouvelles initiatives éthiques puissent voir le jour, et qu'il existe différentes méthodes pour ce faire. Comme ces approches ne s'excluent pas mutuellement dans leur contribution à la confiance publique, il est courant de voir certains pays, comme le Canada et la Nouvelle-Zélande, appliquer simultanément plusieurs méthodes pour veiller au respect de pratiques et comportements éthiques.

Confidentialité et consentement

Le respect de la vie privée est un concept qui s'applique aux personnes concernées, tandis que la confidentialité s'applique aux données elles-mêmes. En ce qui concerne le consentement, il s'agit du concept de « consentement éclairé » : la personne dont les données sont recueillies est consciente du but de la collecte des données et accepte de fournir à cette fin des données qui la concernent (OCDE, 2016[32]). Il s'agit assurément d'un domaine prioritaire, car il est très probable que les citoyens réprouvent la violation de leur vie privée et de leur consentement, surtout pour ce qui est des données sensibles. Ils ne sont pas

toujours conscients de l'intérêt qu'ils ont à rendre accessibles les données qui les concernent, comme indiqué au chapitre 3, et ils peuvent craindre d'être « surveillés » par l'État.

Par conséquent, la non-prise en compte du respect de la vie privée et du consentement peut susciter des tensions et des problèmes. Il s'est avéré par exemple que la clinique Moorfields Eye Hospital et DeepMind, qui s'étaient associés pour explorer des solutions fondées sur l'IA visant à améliorer le suivi ophtalmologique des patients, avaient commis de graves violations de contrat, comme le traitement et le stockage de données sur des sites ne figurant pas dans l'accord de partage des données, le partage de données avec des tierces parties sans consentement clairement donné, ou encore plusieurs défauts de sécurité et de procédures opérationnelles (PrivSec Report, 2019[33]). De tels incidents peuvent nuire à la réputation de ces établissements, qui risquent ainsi de perdre la confiance de leurs patients actuels et potentiels.

C'est pourquoi les pays ont établi des exigences formelles, y compris par voie législative, pour protéger les citoyens tout au long du cycle de collecte, de stockage, de partage et de traitement des données, ainsi qu'en matière d'ouverture, de diffusion et de publication de données. Afin de prévenir les problèmes de non-respect de la vie privée et du consentement, certains pays ont établi des droits en matière de données applicables aux entreprises et aux citoyens. Plus précisément, ils offrent aux citoyens :

- le droit de savoir quelles données les entités publiques détiennent à leur sujet ;
- le droit de savoir quels organismes publics ont un droit d'accès à leurs données ;
- le droit de savoir quels organismes publics ont utilisé leurs données et à quelles fins ;
- le droit de savoir quels organismes publics ont déposé une requête concernant leurs données ;
- le droit de fournir leurs données (personnelles) une seule et unique fois à l'administration ;
- le droit d'accepter ou de refuser que les données qu'ils ont fournies à une institution publique soient partagées avec d'autres entités et réutilisées par elles.

Le **Canada** et le **Royaume-Uni** appliquent systématiquement cette méthode tant aux citoyens qu'aux entreprises. Ces pays ont mis en place des dispositifs concrets qui permettent aux citoyens et aux entreprises d'exercer leur droit de savoir quelles données les entités publiques détiennent à leur sujet. Au Royaume-Uni, ce dispositif est régi par la législation sur la liberté de l'information, tandis qu'au Canada, il entre dans le cadre des lois sur la protection de la vie privée et sur l'accès à l'information.

De même, en **Corée**, il existe des droits en matière de données pour les citoyens comme pour les entreprises, à l'exception du droit de savoir quels organismes publics ont un droit d'accès à leurs données, qui ne concerne que les citoyens. Ainsi, les entreprises ne sont pas en mesure de déterminer quelles organisations publiques ont le droit d'accéder à leurs données. La loi sur la protection des données personnelles (National Law Information Center, 2019[34]) énumère les principes régissant la collecte, le traitement et le partage des informations personnelles. La loi sur la promotion de la fourniture et de l'utilisation des données publiques (loi sur les données ouvertes) (National Law Information Center, 2019[35]) établit, quant à elle, les principes d'une approche éthique du partage, de l'accessibilité et de la réutilisation des données. À eux deux, ces textes visent à assurer un accès universel à l'utilisation des données, l'égalité dans l'accès aux données et l'interdiction des activités empêchant l'utilisation des données publiques.

En mai 2018, le règlement général sur la protection des données (RGPD) est entré en vigueur dans tous les pays de l'UE ; il vise à protéger les citoyens européens contre la violation de leur vie privée et de leurs données. Bien que très semblable aux lois précédentes sur la protection des données, ce règlement a durci les conditions du consentement, ce qui signifie que les entreprises ne peuvent plus utiliser les données d'un citoyen qui n'a pas expressément donné son consentement à cette fin. Il prévoit aussi que le consentement doit être donné sous une forme claire et aisément accessible, avec option de retrait. Par ailleurs, ce règlement donne de larges droits aux personnes concernées, comme le droit d'accès aux données, le droit de rectification, le droit à l'oubli, le droit à la limitation du traitement et le droit à la

portabilité des données (encadré 4.5) (EU GDPR.ORG, 2019[36]). Depuis que le RGPD est entré en vigueur dans l'ensemble de l'UE, les pays européens donnent collectivement suite à la question du respect de la vie privée en transposant les directives de l'UE dans leur droit national.

Au **Portugal**, les citoyens et les entreprises ont la possibilité de faire une requête sur des données et, dans certains cas précis, ils peuvent accepter ou refuser que les données qu'ils ont fournies à une institution publique soient partagées avec d'autres entités publiques et réutilisées par elles.

En **Espagne**, les citoyens ont, depuis 2015, le droit de savoir quelles données les organisations publiques détiennent à leur sujet. Ils ont le droit de connaître toutes ces informations, à tout moment, ainsi que le statut du traitement des procédures qui les concernent. De plus, les citoyens ont un droit de copie des documents visés par les procédures en question. Le RGPD a renforcé l'obligation de consentement pour le traitement des données. La disponibilité de ces données est strictement limitée à celles qui sont demandées aux citoyens par d'autres administrations pour des actes entrant dans leur champ de compétence, conformément aux règles applicables à celles-ci.

Encadré 4.5. Règlement général sur la protection des données : droits de la personne concernée

Droit d'accès – Le règlement général sur la protection des données (RGPD) de l'Union européenne a élargi les droits des personnes concernées par les données, leur offrant notamment le droit d'avoir confirmation, auprès du responsable du traitement des données, que des données à caractère personnel les concernant sont ou ne sont pas traitées et, le cas échéant, où et à quelle fin. De plus, le responsable du traitement fournit gratuitement une copie de ces données sous forme électronique. Il s'agit là d'une évolution spectaculaire en faveur de la transparence des données et de l'autonomie offerte aux citoyens.

Droit de rectification – La personne concernée a le droit d'obtenir la rectification des données à caractère personnel la concernant qui sont inexactes. Sous réserve des finalités du traitement, la personne concernée a le droit d'obtenir que ses données incomplètes soient mises à jour, y compris en fournissant une déclaration complémentaire.

Droit à l'effacement – Également connu sous le nom de « droit à l'oubli », ce droit permet à une personne d'obtenir du responsable du traitement qu'il efface des données à caractère personnel la concernant, qu'il cesse toute diffusion de ces données et, éventuellement, qu'il demande aux tierces parties de cesser de traiter ces données. Les motifs d'effacement sont notamment le fait que les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées et traitées, ou que la personne concernée a retiré son consentement. Lorsqu'il traite une telle demande, le responsable du traitement doit mettre en balance les droits de la personne concernée et d'éventuels motifs d'intérêt public justifiant la disponibilité des données.

Droit à la limitation du traitement – Un individu peut demander à une organisation de limiter l'utilisation de ses données personnelles lorsqu'il a une raison particulière de le faire. Ce peut être parce qu'il conteste l'exactitude des informations détenues ou la manière dont ses données sont traitées. Dans la plupart des cas, il ne pourra pas demander la limitation du traitement de ses données pour une durée indéfinie, mais la limitation pourra rester en place pendant un certain temps.

Droit à la portabilité des données – Le RGPD a instauré la portabilité des données, c'est-à-dire le droit pour une personne d'obtenir les données qui la concernent et qu'elle a préalablement fournies, dans un format couramment utilisé et lisible sur un ordinateur, afin de pouvoir les transmettre à un autre responsable de traitement des données.

Source : EU GDPR.ORG (2019[41]), GDPR Key Changes, https ://eugdpr.org/the-regulation.

Avant l'entrée en vigueur du RGPD, le droit d'accès était quelque peu limité dans certains pays européens. Au **Danemark** et en **Suède**, par exemple, ces droits n'étaient pas très étendus. Le Danemark n'offrait qu'un droit aux citoyens et aux entreprises, celui d'accéder aux données que les organismes publics détenaient à leur sujet. Ce droit existait aussi en Suède, où les citoyens avaient également le droit de savoir quels organismes publics pouvaient accéder à leurs données. Dans certains cas, le Danemark permettait aux citoyens de savoir quelles données les entités publiques détenaient à leur sujet, grâce aux sites web www.borger.dk et www.sundhed.dk. De plus, le Programme des données de base avait établi le principe selon lequel les citoyens et les entreprises n'étaient tenus de fournir leurs données personnelles qu'une seule et unique fois à l'administration, laquelle était donc censée les partager et les réutiliser.

La mise en conformité de tous les pays de l'UE avec la nouvelle législation a incité des États non européens à emprunter cette voie. Ainsi, juste après l'entrée en vigueur du RGPD, le **Japon** a signé un accord avec l'Union européenne aux fins d'une reconnaissance réciproque d'un niveau adéquat de protection des données à caractère personnel. Le Japon est le premier pays à bénéficier, de la part de la Commission européenne, d'une telle décision qui non seulement fluidifie les échanges de données entre le Japon et l'UE, mais aussi facilite les transferts de gros volumes de données, les échanges et les partenariats en la matière (PrivSec Report, 2019[37]).

Bien que le champ couvert par les droits en matière de données varie d'un pays à l'autre, la mise en œuvre du RGPD a braqué les projecteurs sur les droits des individus et des entreprises à l'égard de leurs données. Avant l'entrée en vigueur de ce règlement, le droit d'accès aux données était plus ou moins bien couvert dans les différents pays. Qui plus est, le RGPD a instauré, outre le droit d'accès, le droit de rectification, le droit à l'effacement et le droit à la limitation du traitement, qui contribuent grandement à nourrir la confiance du public.

Transparence

La transparence est un environnement dans lequel sont mis à la disposition du public, sous une forme compréhensible, accessible et actualisée : les objectifs des politiques publiques ; leur cadre juridique, institutionnel et économique ; les décisions prises par les pouvoirs publics et leur justification ; les données et informations relatives aux politiques monétaires et financières ; et les modalités de redevabilité des organismes publics (OCDE, 2019[38]).

Comme les administrations publiques commencent à intégrer les technologies émergentes dans leurs processus de décision, les données utilisées pour alimenter les systèmes d'IA jouent un rôle essentiel. Bien souvent, cependant, les citoyens ne savent pas quelles données sont utilisées, comment et par qui (Saidot, 2019[39]). C'est pourquoi la transparence des données assure la haute qualité et la fiabilité des données (OCDE, à paraître[40]), ce qui est fondamental pour une bonne mise en œuvre de l'apprentissage machine et d'autres applications de l'IA, et pour le maintien de la confiance.

Tandis que les pays envisagent le rôle que l'IA peut jouer pour prendre en charge les activités de prise de décision des fonctionnaires, il est nécessaire d'étudier comment les administrations pourraient procéder à un examen de leurs processus de prise de décision et en analyser les conclusions, lesquelles ont une incidence sur la vie des citoyens. Il est donc important que les pays prennent des mesures pour rendre transparents leurs algorithmes de prise de décision.

Exposer « l'envers » d'un algorithme est un puissant moyen de renforcer la confiance des usagers, de corriger les erreurs et d'éviter les biais. La transparence des algorithmes peut non seulement contribuer à l'amélioration de la communauté de l'IA, mais aussi imposer le respect des droits individuels eu égard aux données, qui signifie, aux termes du RGPD, que les individus ont le droit d'être informés de la collecte et de l'utilisation de données les concernant, ainsi que, de façon détaillée, de l'existence d'une prise de décision automatisée, y compris d'un profilage (Information Commissioner's Office, 2019[41]).

En France, la loi Lemaire a été adoptée à cette fin en 2016 pour une plus grande transparence. Elle vise à instaurer un service public des données digne de confiance en encourageant l'innovation et en bâtissant un cadre de confiance qui garantisse les droits des usagers tout en protégeant leurs données personnelles (Dreyfus, 2019[42]).

Au **Royaume-Uni**, le Cadre pour l'éthique en matière de données constitue le fondement des travaux menés dans le domaine de la science des données ; en particulier, son Principe n°6 affirme que toutes les activités devraient être menées de façon aussi ouverte et redevable que possible (Ministère britannique du Numérique, 2019[30]). Si ce cadre n'a pas de vocation prescriptive formelle, il s'inscrit dans la lignée de la méthode suivie par le Royaume-Uni pour diffuser les bonnes pratiques dans l'ensemble du secteur public, aux termes de la norme de service public et du manuel des services. À l'appui de ce cadre, le bureau britannique pour l'intelligence artificielle a été chargé d'explorer l'utilisation des algorithmes et d'autres techniques telles que l'apprentissage machine aux fins de la transformation de l'administration et de l'aide à la prise de décision. Le gouvernement britannique collabore aussi avec des établissements universitaires et de recherche de l'industrie, comme le *Alan Turing Institute*, l'*Open Data Institute*, la *Open Government Partnership* et le *Policy Lab*.

La **Nouvelle-Zélande** a récemment formulé des principes pour l'utilisation sûre et efficace des données et de l'analytique, qui visent à proposer de bonnes pratiques et à aider les organismes utilisant les algorithmes dans leur prise de décision. Ces principes ont également pour objet d'informer les citoyens et de leur inspirer confiance dans la manière dont l'administration exploite les algorithmes (Gouvernement de la Nouvelle-Zélande, 2019[43]).

En **Corée**, l'initiative « projets d'analyse des données massives du secteur public » encourage, depuis 2014, une gestion scientifique et fondée sur les données de l'administration centrale, des administrations locales et des institutions publiques.

Même si les administrations publiques établissent des cadres ou des principes pour normaliser l'information et clarifier la communication et l'usage des données aux fins d'accentuer la transparence, une autre manière de gagner la confiance des citoyens consiste pour elles à se montrer ouvertes à un examen minutieux de leur performance publiée, en faisant aussi entrer cette ouverture dans leur culture ordinaire ainsi que dans les normes et principes démocratiques.

De fait, certains pays font appel à la transparence en tant qu'outil concret et accompagnent leurs approches numériques de dispositifs pratiques permettant aux citoyens de comprendre comment leurs données sont utilisées, ce qui les aide à découvrir l'action menée par les autorités pour renforcer la confiance (OCDE, 2019[44]). Offrir la maîtrise des données ou montrer comment les données sont exploitées sont des démarches importantes pour gagner la confiance des citoyens dans les services publics, et donc dans l'administration.

En ce qui concerne l'identité numérique, l'Espagne, avec *Carpeta Ciudadana*, et le Danemark, avec *NemID*, offrent à leurs citoyens la possibilité de maîtriser les données qui les concernent ainsi que la capacité de voir, en détail, comment leurs données sont extraites et utilisées en ligne (OCDE, 2019[44]). De plus en plus, les pays offrent aux citoyens l'accès à un site web où ils peuvent non seulement découvrir leur propre activité de connexion et la manière dont les organisations utilisent leurs données, mais aussi accorder et retirer l'autorisation d'utiliser leurs données.

Sécurité

Par sécurité, on entend les mesures prises pour prévenir un accès ou un usage non autorisé des données (OCDE, 2019[38]). La gestion des données dans l'administration est importante, d'une part, eu égard à la manière dont elle peut être appliquée et exploitée pour concevoir de meilleures politiques et améliorer les services et, d'autre part, selon comment elle est employée pour protéger la vie privée des citoyens et préserver leur confiance. Les citoyens ont besoin de savoir que des efforts sont déployés afin que leur vie

privée soit respectée, et qu'ils peuvent faire confiance à l'administration pour traiter leurs informations personnelles et les protéger des risques potentiellement associés au traitement de ces données par les pouvoirs publics.

Si, dans l'ensemble du monde, les correctifs ne sont pas apportés aux ordinateurs, cela peut avoir des effets dévastateurs pour le secteur privé comme pour le secteur public. Les attaques informatiques peuvent être extrêmement coûteuses, non seulement sur le plan financier, mais aussi sur le plan de la réputation des organisations qui en sont victimes. Celles-ci peuvent perdre la confiance des utilisateurs actuels et potentiels de leurs services (IT Governance, 2019[45]).

De fait, la perspective d'atteintes à la sécurité numérique qui paralysent les infrastructures et empêchent les citoyens d'accéder aux services n'est pas un risque hypothétique mais une réalité. En mai 2017, l'attaque du logiciel malveillant WannaCry a touché des entreprises et des particuliers dans plus de 150 pays, y compris FedEx, Renault-Nissan et le Service national de santé du Royaume-Uni (NHS). Le mois suivant, l'attaque de NotPetya a causé des dommages estimés à 10 milliards de dollars. Ces deux attaques ont exploité un outil de pénétration dénommé EternalBlue, qui avait été créé, et divulgué, par l'Agence nationale de sécurité des États-Unis. Si l'installation d'un correctif de protection contre EternalBlue aurait atténué l'impact de WannaCry, l'évolution de NotPetya signifie que ce logiciel était capable d'infecter même des ordinateurs protégés. Ces événements soulignent néanmoins combien il est important que les administrations publiques, les entreprises et les citoyens prennent au sérieux la sécurité de leurs données (Welby, 2019[20]).

Ainsi, la sécurité numérique n'est pas une option : elle doit être considérée comme un volet fondamental des stratégies publiques en matière de numérique, de données et de technologies. Il convient de l'assurer selon des modalités qui permettent aux pouvoirs publics de faire une utilisation proactive des données pour concevoir et faire fonctionner une administration de meilleure qualité. Comme le prévoit le RGPD, les organisations doivent faire de la sécurité numérique une priorité, en appliquant des mesures techniques et organisationnelles appropriées afin de protéger les données qu'elles détiennent. À défaut, elles s'exposent à de lourdes amendes (IT Governance, 2019[45]).

De nombreux pays ont placé la sécurité numérique parmi les premières priorités de leur programme d'administration numérique. C'est pourquoi ils sont nombreux à avoir élaboré des stratégies et des politiques pour gérer les risques de sécurité auxquels sont exposées les données et les informations publiques. Des pays tels que la **Corée** et le **Royaume-Uni** ont une stratégie de sécurité numérique autonome, tandis que, pour l'**Irlande**, il s'agit d'une stratégie complémentaire.

La **Corée** a mis sur pied une politique autonome qui est centrée sur les bonnes pratiques en matière d'utilisation et de réglementation des données, visant à écarter les menaces contre la sécurité numérique. Le Service national des ressources en information gère tous les serveurs et bases de données de l'État aux termes de cette politique de sécurité, plaçant ainsi la question sous la supervision d'une instance centrale.

Le **Royaume-Uni** a non seulement inscrit la sécurité numérique dans un chapitre spécial de sa stratégie numérique nationale, mais en a fait également une Stratégie nationale pour la cybersécurité 2016-2021. Ces deux documents affichent l'ambition de faire du Royaume-Uni le lieu le plus sûr au monde pour vivre et travailler en ligne. Le Centre national pour la cybersécurité se propose de nouer des partenariats effectifs entre l'État, les professionnels et le grand public afin de renforcer la sécurité en ligne du pays. Il propose des réponses aux cyberincidents ainsi qu'un lien vers les services de sécurité du Royaume-Uni, et représente la voix nationale faisant autorité en matière de cybersécurité. Pour la première fois, les employés des secteurs public comme privé se voient indiquer une voie à suivre pour collaborer directement avec les professionnels de la cybersécurité et accéder ainsi aux meilleurs conseils et aides possibles en vue de sécuriser les réseaux et systèmes contre les menaces d'atteinte à la sécurité numérique.

Bien que l'**Irlande** n'ait pas adopté une stratégie autonome, elle a fait de la sécurité numérique une priorité de son programme d'action publique, puisque c'est l'un des cinq piliers de sa Stratégie informatique pour le service public.

Néanmoins, la sécurité numérique est un domaine qui est déjà, dans les différents pays, soit une stratégie autonome soit un point dans un programme d'action plus large, mais il est tout aussi important de doter le grand public de compétences en matière de sécurité numérique. Investir dans l'acquisition de ces compétences est également une nécessité, non seulement pour la protection de l'administration, mais aussi pour donner aux citoyens les connaissances dont ils ont besoin pour assurer leur propre sécurité, afin qu'ils soient plus vigilants dans le cadre de leurs interactions en ligne et face à l'utilisation de leurs données personnelles.

Dans le monde entier, des organisations ont constaté que, dans différents secteurs, les compétences en matière de sécurité numérique accusaient des lacunes. Un rapport de McAfee affirmait ainsi que 82 % des pays interrogés (Allemagne, Australie, États-Unis, France, Israël, Japon, Mexique et Royaume-Uni) déploraient une pénurie de compétences en matière de sécurité numérique dans leur pays (Center for Strategic and International Studies, 2016[46]). Le gouvernement britannique, quant à lui, a commandé une étude en vue d'évaluer le déficit de compétences techniques de base eu égard à la sécurité numérique, qui a permis de constater que 54 % des organisations du secteur privé et sans but lucratif, ainsi que 18 % des organismes publics, souffraient d'un tel déficit (Ministère britannique du Numérique, 2019[47] ; Pedley et al., 2018[48]). Compte tenu des rapides avancées de la technologie, de l'économie numérique et des menaces dans ce domaine, l'existence d'un déficit aussi vaste devient un problème pressant. Bien qu'il soit très difficile d'appréhender la nature et l'évolution des compétences en matière de sécurité numérique au fil du temps, des pays comme le Royaume-Uni ont commencé à se pencher sur cette question, comme en témoigne sa Stratégie nationale pour la cybersécurité, examinée à l'encadré 4.6 (Ministère britannique du Numérique, 2019[47]).

Encadré 4.6. Le Royaume-Uni renforce ses capacités en matière de cybersécurité

À l'origine, le Royaume-Uni a mis sur pied une stratégie nationale pour la cybersécurité afin de pouvoir disposer durablement d'une réserve de spécialistes nationaux de la cybersécurité, capables de répondre aux exigences croissantes d'une économie de plus en plus numérique, dans les secteurs public et privé ainsi que dans la défense. Cependant, face à la demande croissante de compétences en la matière, cette stratégie se propose d'aller beaucoup plus loin.

Le gouvernement a pour ambition de remédier au déficit plus général de capacités en matière de cybersécurité en veillant à ce que : des professionnels correctement qualifiés soient présents dans la population active aujourd'hui et à l'avenir ; les organisations et leur personnel aient les moyens de gérer efficacement les risques de cybersécurité ; et les citoyens soient conscients de la valeur de leurs données personnelles et capables de pratiquer une « cyber-hygiène » de base pour se protéger eux-mêmes et protéger les organisations qui les emploient.

Cette stratégie a donc pour mission de renforcer les capacités de cybersécurité dans tous les secteurs afin que le Royaume-Uni dispose du niveau et de la gamme de compétences nécessaires pour maintenir la résilience face aux cybermenaces et devienne le leader mondial de l'économie numérique.

Pour accomplir cette mission, elle veillera à faire en sorte que :

- le Royaume-Uni dispose d'un corps de métier bien structuré et abordable qui représente, défend et porte l'excellence dans les différentes spécialités de la cybersécurité, et qui soit durable et réactif au changement ;

- le Royaume-Uni abrite des systèmes d'éducation et de formation qui offrent les fondements adéquats pour repérer, former et placer les nouveaux talents, non encore exploités, en matière de cybersécurité ;
- la population active du Royaume-Uni dispose de la gamme et du niveau de compétences nécessaires à une économie numérique réellement sûre, où les organisations basées au Royaume-Uni, dans tous les secteurs, soient à même de prendre des décisions éclairées quant à la gestion de leurs risques en matière de cybersécurité ;
- le Royaume-Uni demeure un leader mondial de la cybersécurité, ayant accès aux meilleurs talents, avec un secteur public qui donne l'exemple en développant ses capacités de cybersécurité.

Source : Department for Digital, Culture, Media & Sport (2019[52]), Initial National Cyber Security Skills Strategy: Increasing the UK's Cyber Security Capability - A Call for Views, Executive Summary, https://www.gov.uk/government/publications/cyber-security-skills-strategy/initial-national-cyber-security-skills-strategy-increasing-the-uks-cyber-security-capability-a-call-for-views-executive-summary#fn:1

Lignes directrices pour l'éthique en matière de données

Face à l'universalité des problèmes à résoudre et des défis à relever, les pays du monde entier ont commencé à envisager de mutualiser de bonnes pratiques pour mettre sur pied des cadres éthiques en vue d'élaborer un ensemble commun de principes. Cela contribuerait à forger une culture plus solide de l'usage éthique des données dans tous les pays. C'est là une préoccupation extrêmement pertinente parce que, dans un monde de plus en plus numérique, les flux et partages de données entre pays sont considérés comme un moyen d'améliorer la fourniture de services à des citoyens mondialisés et de renforcer la collaboration internationale pour lutter contre des problèmes communs. Le Groupe thématique de l'OCDE sur le secteur public axé sur les données offre un exemple de ces initiatives conjointes (encadré 4.7).

Formulées à l'intention des décideurs publics, des statisticiens, des analystes, des spécialistes des données et de tous les agents publics qui traitent des données, les orientations visent à encourager les fonctionnaires à collaborer pour concevoir un usage approprié des données. Les orientations éthiques proposées, présentées à l'encadré 4.7, constituent une réponse en matière de comportements éthiques, de droits numériques et de droits relatifs aux données. Bien que les lois et règlements afférents aux droits des citoyens, le comportement des fonctionnaires et l'application des données et des technologies éclairent déjà l'activité de l'administration, il est nécessaire d'accompagner ces éléments d'orientations éthiques afin d'obtenir des pratiques éthiques, des conduites cohérentes et le maintien de la confiance.

Encadré 4.7. Propositions d'orientations en matière d'éthique des données

Placé sous l'égide des Pays-Bas, le Groupe thématique de l'OCDE sur le secteur public axé sur les données est convenu, en juin 2019, à la cinquième réunion du groupe d'experts, d'adopter les orientations suivantes.

Au sein d'un secteur public axé sur les données, les données et leur utilisation sont au service de l'intérêt général. La collecte et l'usage des données par l'administration doivent renforcer les institutions de la démocratie et l'état de droit.

Les administrations utilisant les données de manière conforme à l'éthique pour améliorer la qualité des services publics et accroître la valeur publique, tout en renforçant les normes démocratiques et en évitant la discrimination, doivent constituer la norme.

L'objectif d'un usage particulier des données doit être clairement exprimé. Il faut s'assurer que l'usage des données répond à un but clairement formulé, qui explique les raisons pour lesquelles les données sont utilisées et qui répond aux préoccupations des différentes parties prenantes.

Toutes les parties au cycle de valeur des données doivent pouvoir comprendre simplement l'objectif, préalablement formulé, de tout usage des données, à chaque stade du processus d'utilisation des données. La manière dont celui-ci est conçu, le but qu'il vise, le besoin auquel il répond et les avantages qu'il est censé procurer doivent être clairs pour toutes les parties concernées, de sorte que le droit à l'information puisse s'appliquer, que la qualité et la confiance soient garanties tout au long du processus et que chaque utilisation des données soit expliquée.

Les limites de l'utilisation des données doivent être définies. Il faut s'assurer que la conception prend en considération une utilisation équilibrée des données en mettant en balance les coûts et avantages sociétaux pertinents avec une norme reposant sur la minimisation des données lorsqu'il s'agit de données à caractère personnel. On assure ainsi la qualité de la conception et la capacité d'expliquer comment les données sont utilisées.

Les administrations doivent définir les limites de l'utilisation des données afin de promouvoir la transparence. Elles doivent collecter et utiliser la quantité juste suffisante de données non biaisées qui leur permet d'accomplir leurs tâches. Toute utilisation abusive des données peut avoir des conséquences négatives, comme la perte de confiance des citoyens dans la fonction publique.

Les données doivent être utilisées avec intégrité. L'administration ne doit pas abuser de sa position, des données à sa disposition ou de la confiance du public.

Les administrations doivent utiliser les données de manière responsable afin de renforcer la confiance. Compte tenu des opportunités et de l'intérêt que peuvent présenter les données, une transition stratégique de l'administration vers une approche centrée sur les données place le processus de conception et de prestation des services publics au centre de l'attention. Comme les données utilisées par l'administration pour améliorer la qualité des services sont de nature hautement sensible, ce processus nécessite non seulement une attention soigneuse mais aussi un traitement sécurisé et un comportement éthique de la part des agents publics qui traitent ces données.

Il faut rendre compte de ses actions. Les administrations créent des mécanismes qui permettent aux citoyens de comprendre et d'autoriser l'utilisation de leurs données personnelles, en organisant la redevabilité interne et externe. Les parties prenantes doivent savoir à qui adresser leurs questions, remarques ou erreurs, et les administrations doivent être réactives face aux informations fournies par les citoyens.

Rendre compte, pour une administration, ce n'est pas simplement expliquer comment les données personnelles sont traitées et divulguer les données publiques, mais c'est aussi être transparente quant aux activités administratives et appliquer une sécurité numérique suffisamment rigoureuse pour protéger les données détenues par l'administration. Cela permet aux citoyens d'avoir davantage confiance et de constater leur contribution aux services publics.

L'administration doit être compréhensible et transparente. La transparence concerne la manière dont les données sont recueillies et utilisées, et consiste aussi à communiquer clairement et de façon compréhensible quant au rôle des données, y compris des algorithmes, dans la fourniture de biens et services publics. Les données détenues par l'administration sont des données ouvertes, sauf en cas de préoccupations légitimes relevant de la vie privée, de questions économiques ou de la sécurité.

Chaque fois qu'elle utilise des données, l'administration doit être transparente et communiquer avec efficience l'objectif de cette utilisation et la manière dont les données sont traitées. Le droit à l'information est un droit fondamental en matière de données parce qu'il contribue à une communication claire et transparente entre les administrations et les citoyens et qu'il favorise l'autonomie de ces derniers, ce qui est essentiel pour nourrir leur confiance envers l'administration.

La maîtrise de leurs données personnelles par les citoyens doit être élargie. Lorsqu'ils acquièrent des connaissances permettant de prendre des décisions quant au partage de leurs données personnelles à l'intérieur ou à l'extérieur de l'administration, les citoyens sont plus autonomes et ont davantage de perspectives d'action.

En autonomisant les citoyens par une meilleure maîtrise de leurs données personnelles, les administrations font la preuve qu'elles placent les citoyens au centre et qu'elles valorisent leur participation. Ils jouissent ainsi du droit d'être informé quant à leurs données, d'y accéder, et de les modifier, supprimer ou limiter, du droit à la portabilité des données, du droit de formuler des objections ainsi que de droits liés à la prise de décision automatisée.

La discrimination doit être évitée et l'inclusion encouragée. L'utilisation appliquée des données doit reconnaître, et atténuer, tout biais potentiel de sorte qu'il ne conduise jamais à la discrimination : les personnes placées dans des cas similaires doivent toujours être traitées de la même façon.

Afin de traiter les données de manière responsable et d'éviter les données biaisées, les fonctionnaires doivent posséder les compétences techniques nécessaires pour repérer les erreurs et les situations biaisées.

Références

Aberbach, J. (2007), « Citizens and consumers », *Public Management Review*, vol. 7/2, pp. 225-246, http://dx.doi.org/10.1080/14719030500091319. [9]

Ahn, S. et P. Hemmings (2000), « Policy Influences on Economic Growth in OECD Countries: An Evaluation of the Evidence », *Documents de travail du Département des affaires économiques de l'OCDE*, n° 246, Éditions OCDE, Paris, https://dx.doi.org/10.1787/581718238837. [4]

Asamblea Nacional (2019), *Ley 81 de 26 de marzo de 2019 - De protección de datos personales*, https://www.gacetaoficial.gob.pa/pdfTemp/28743_A/GacetaNo_28743a_20190329.pdf. [18]

Asamblea Nacional (2012), *Ley 83 de 9 de Noviembre de 2012 - Regula el uso de medios electrónicos para los tramites gubernamentales*, http://www.innovacion.gob.pa/descargas/Ley_83_del_9_de_noviembre_2012.pdf. [16]

Australian National Data Service (2019), *Indigenous Data*, https://www.ands.org.au/working-with-data/sensitive-data/indigenous-data. [28]

Center for Strategic and International Studies (2016), *Hacking the Skills Shortage: A Study of the International Shortage in Cybersecurity Skills*, McAfee, https://www.mcafee.com/content/dam/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf. [46]

Commission européenne (2019), *Digital Single Market*, Commission européenne, https://ec.europa.eu/digital-single-market/en. [15]

Data Protection Commission (2019), *The Data Protection Commission*, https://www.dataprotection.ie. [27]

Department for Digital, Culture, Media & Sport (2018), *Guidance Data Ethics Framework*, Department for Digital, Culture, Media & Sport, Londres, https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework#the-data-ethics-framework-principles. [51]

Dreyfus (2019), *France : Service public et traitement des données personnelles*, Dreyfus, https://dreyfus.fr/2019/08/05/service-public-et-traitement-des-donnees-personnelles/. [42]

EU GDPR.ORG (2019), *GDPR Key Changes*, https://eugdpr.org/the-regulation. [36]

Floridi, L. et M. Taddeo (2016), « What is data ethics? », *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 374, http://dx.doi.org/10.1098/rsta.2016.0360. [11]

Freedom House (2018), *Mexico*, https://freedomhouse.org/report/freedom-net/2018/mexico. [14]

Gouvernement de la Corée (2019), *Personal Information Protection Commission*, http://www.pipc.go.kr/cmt/main/english.do. [19]

Gouvernement de la Nouvelle-Zélande (2019), *Algorithm Review Underway to Increase Transparency and Accountability*, https://www.data.govt.nz/blog/algorithm-review-underway-to-increase-transparency-and-accountability/. [43]

Gouvernement du Canada (2019), *Évaluation de l'incidence algorithmique (EIA)*, https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/technologiques-modernes-nouveaux/utilisation-responsable-ai/evaluation-incidence-algorithmique.html. [31]

Gouvernement du Canada (2019), *Utilisation responsable de l'intelligence artificielle (IA)*, https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/technologiques-modernes-nouveaux/utilisation-responsable-ai.html. [49]

Healy, B. (2012), *Centre de gouvernance de l'information des Premières Nations de l'Alberta*, Centre de gouvernance de l'information des Premières Nations de l'Alberta, Alberta, https://www.fnhma.ca/archive/conference/2012/files/Bonnie_Healy.pdf. [29]

Information Commissioner's Office (2019), *Right To Be Informed*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/. [41]

IT Governance (2019), *What is Cybersecurity?*, https://www.itgovernance.co.uk/what-is-cybersecurity. [45]

Korean Ministry of Public Administration and Security (2019), *10 Commandments to Prevent Misuse of Personal Information*, https://www.privacy.go.kr/nns/ntc/cmd/tenCommandments.do. [24]

Korean Ministry of the Interior and Safety (2019), *Personal Data Protection Laws in Korea*, https://www.privacy.go.kr/eng. [23]

McKnight, D. et N. Chervany (2000), « What is trust? A conceptual analysis and an interdisciplinary model », *AMCIS 2000 Proceedings*, vol. 382, http://aisel.aisnet.org/amcis2000/382. [1]

Ministère britannique du Numérique, D. (2019), *Guidance Data Ethics Framework*, Ministère britannique du Numérique, de la Culture, des Médias et des Sports, Londres, https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework. [30]

Ministère britannique du Numérique, D. (2019), *Initial National Cyber Security Skills Strategy: Increasing the UK's Cyber Security Capability - A Call for Views, Executive Summary*, Department for Digital, Culture, Media & Sport, Londres, https://www.gov.uk/government/publications/cyber-security-skills-strategy/initial-national-cyber-security-skills-strategy-increasing-the-uks-cyber-security-capability-a-call-for-views-executive-summary#fn:1. [47]

Ministerio de la Presidencia (2017), *Decreto ejecutivo 511 de 24 de noviembre de 2017 - Adopta la politica pública de transparência de datos abiertos de gobierno*, https://www.gacetaoficial.gob.pa/pdfTemp/28421/GacetaNo_28421_20171207.pdf. [17]

Murtin, F. et al. (2018), « Trust and its determinants: Evidence from the Trustlab experiment », *OECD Statistics Working Papers*, n° 2018/2, Éditions OCDE, Paris, https://dx.doi.org/10.1787/869ef2ec-en. [5]

National Law Information Center (2019), *Law by classification*, http://www.law.go.kr/LSW/eng/engLsSc.do?menuId=1&query=%EA%B3%B5%EA%B3%B5%EB%8D%B0%EC%9D%B4%ED%84%B0&x=0&y=0#liBgcolor0. [35]

National Law Information Center (2019), *Law by Classification*, http://www.law.go.kr. [34]

New Zealand Ministry of Foreign Affairs and Trade (2019), *Christchurch Call*, https://www.christchurchcall.com/call.html. [53]

New Zealand Ministry of Social Development (2019), *Using Personal Information Responsibly*, https://www.msd.govt.nz/about-msd-and-our-work/work-programmes/initiatives/phrae/index.html. [50]

OCDE (2019), *Digital Government in Chile – Digital Identity*, OECD Digital Government Studies, Éditions OCDE, Paris, https://dx.doi.org/10.1787/9ecba35e-en. [44]

OCDE (2019), *Digital Government Review of Panama: Enhancing the Digital Transformation of the Public Sector*, OECD Digital Government Studies, Éditions OCDE, Paris, https://dx.doi.org/10.1787/615a4180-en. [13]

OCDE (2019), *Digital Government Review of Sweden: Towards a Data-driven Public Sector*, OECD Digital Government Studies, Éditions OCDE, Paris, https://dx.doi.org/10.1787/4daf932b-en. [10]

OCDE (2019), *OECD Glossary of Statistical Terms*, OCDE, Paris, https://stats.oecd.org/glossary. [38]

OCDE (2018), *Comment va la vie ? 2017 : Mesurer le bien-être*, Éditions OCDE, Paris, https://dx.doi.org/10.1787/how_life-2017-fr. [6]

OCDE (2017), *Panorama des administrations publiques 2017*, Éditions OCDE, Paris, https://dx.doi.org/10.1787/gov_glance-2017-fr. [2]

OCDE (2017), *Trust and Public Policy: How Better Governance Can Help Rebuild Public Trust*, Examens de l'OCDE sur la gouvernance publique, Éditions OCDE, Paris, https://dx.doi.org/10.1787/9789264268920-en. [8]

OCDE (2016), « Research Ethics and New Forms of Data for Social and Economic Research », *OECD Science, Technology and Industry Policy Papers*, n° 34, Éditions OCDE, Paris, https://dx.doi.org/10.1787/5jln7vnpxs32-en. [32]

OCDE (à paraître), *Digital Government Review of Chile*, Éditions OCDE, Paris. [21]

OCDE (à paraître), *State of the Art on Emerging Technologies*, OCDE, Paris, à paraître. [40]

OCDE/KDI (2018), *Understanding the Drivers of Trust in Government Institutions in Korea*, Éditions OCDE, Paris, https://dx.doi.org/10.1787/9789264308992-en. [7]

ODI (2017), *Ethical Data Handling*. [22]

Pedley, D. et al. (2018), *Understanding the UK Cybersecurity Skills Labour Market*, Ipsos MORI Social Reearch Institute, https://www.ipsos.com/sites/default/files/ct/publication/documents/2019-01/understanding_the_uk_cyber_security_skills_labour_market.pdf. [48]

Powles, J. et H. Hal (2018), *Response to DeepMind*. [25]

PrivSec Report (2019), *European Commission Adopts Adequacy Decision on Japan, Creating the World's Largest Area of Safe Data Flows*, Data Protection World Forum Ltd, https://gdpr.report/news/2019/01/24/european-commission-adopts-adequacy-decision-on-japan-creating-the-worlds-largest-area-of-safe-data-flows/. [37]

PrivSec Report (2019), *NHS Patient Data Used by Google Without Consent*, Data Protection World Forum Ltd, https://gdpr.report/news/2019/09/19/privacy-nhs-patient-data-used-by-google-without-consent. [33]

Putman, R., R. Leonardi et R. Nanetti (1993), *Making Democracy Work*, Princeton University Press. [3]

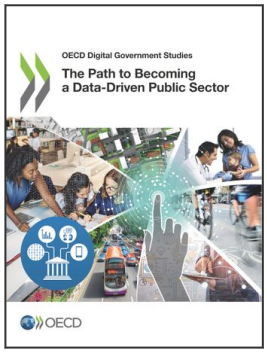
Saidot (2019), *A Consortium of Finnish Organisations Seeks for a Shared Way to Proactively Inform Citizens on AI Use*, Saidot, Espoo, Finlande, https://www.saidot.ai/post/a-consortium-of-finnish-organisations-seeks-for-a-shared-way-to-proactively-inform-citizens-on-ai-use. [39]

Stats NZ (2019), *Data Ethics Advisory Group*, https://www.data.govt.nz/about/government-chief-data-steward-gcds/data-ethics-advisory-group (consulté le 27 août 2019). [52]

van Ooijen, C., B. Ubaldi et B. Welby (2019), « A data-driven public sector: Enabling the strategic use of data for productive, inclusive and trustworthy governance », *Documents de travail de l'OCDE sur la gouvernance publique*, n° 33, Éditions OCDE, Paris, https://dx.doi.org/10.1787/09ab162c-en. [12]

Wagner, B. (2018), *Ethics as an Escape from Regulation: From Ethics-washing to Ethics-shopping?*, Amsterdam University Press, https://www.privacylab.at/wp-content/uploads/2018/07/Ben_Wagner_Ethics-as-an-Escape-from-Regulation_2018_BW9.pdf. [26]

Welby, B. (2019), « The impact of digital government on citizen well-being », *Documents de travail de l'OCDE sur la gouvernance publique*, n° 32, Éditions OCDE, Paris, https://dx.doi.org/10.1787/24bac82f-en. [20]



Extrait de :

The Path to Becoming a Data-Driven Public Sector

Accéder à cette publication :
https://doi.org/10.1787/059814a7-en

Merci de citer ce chapitre comme suit :

OCDE (2020), « Le rôle des données dans le renforcement de la confiance des citoyens », dans *The Path to Becoming a Data-Driven Public Sector*, Éditions OCDE, Paris.

DOI: https://doi.org/10.1787/b403fde9-fr

Cet ouvrage est publié sous la responsabilité du Secrétaire général de l'OCDE. Les opinions et les arguments exprimés ici ne reflètent pas nécessairement les vues officielles des pays membres de l'OCDE.

Ce document, ainsi que les données et cartes qu'il peut comprendre, sont sans préjudice du statut de tout territoire, de la souveraineté s'exerçant sur ce dernier, du tracé des frontières et limites internationales, et du nom de tout territoire, ville ou région. Des extraits de publications sont susceptibles de faire l'objet d'avertissements supplémentaires, qui sont inclus dans la version complète de la publication, disponible sous le lien fourni à cet effet.

L'utilisation de ce contenu, qu'il soit numérique ou imprimé, est régie par les conditions d'utilisation suivantes : http://www.oecd.org/fr/conditionsdutilisation.

OCDE