GTSP3 : La protection de la vie privée et la protection des données en tant que droits fondamentaux : exposé de faits

préparé à l'intention du GTSP3 sur la protection de la vie privée et les droits de la personne

Tables des matières

La protection de la vie privée et la protection des données en tant que droits fondamentaux : exposé

À propos du présent document

Le présent document est le fruit des travaux du Groupe de travail sur la stratégie politique – volet 3 (GTSP3) de l'Assemblée mondiale pour la protection de la vie privée (AMVP).

Son mandat consiste à élaborer un exposé mettant en évidence la relation entre la protection de la vie privée et des données et d'autres droits et libertés, en s'appuyant sur la *Résolution internationale sur la protection de la vie privée en tant que droit humain fondamental et condition préalable à l'exercice d'autres droits fondamentaux*, adoptée lors de la Conférence de 2019 de l'AMVP[1].

Pour atteindre cet objectif, le GTSP3 a établi un plan comportant quatre étapes :

1. Recherche et collecte d'information (recherche de faits);
2. Préparation de l'ébauche d'un exposé;
3. Réception de la rétroaction externe sur l'ébauche de l'exposé;
4. Mise au point définitive de l'exposé en vue de son évaluation et de son adoption en 2021.

Nous aimerions remercier nos collègues des autorités en matière de protection des données de toutes les régions du monde qui ont fourni des renseignements cruciaux, circonscrit les études qui ont été menées et offert une réflexion approfondie sur les résultats présentés ci-dessous. Ce travail n'aurait pas été possible sans leur contribution et leur engagement. Mentionnons notamment :

- L'Autorité de réglementation de l'information, Afrique du Sud
- Le Commissaire fédéral à la protection des données et à la liberté d'information, Allemagne
- La Direction nationale de la protection des données personnelles, Argentine
- L'Autorité nationale de protection des données, Belgique
- Le Commissariat à la protection de la vie privée, Canada
- L'Autorité catalane de protection des données, Catalogne
- Le Conseil chilien de la transparence
- Le Conseil de l'Europe
- Le Centre financier international de Dubaï
- La Federal Trade Commission, États-Unis
- Le Bureau d'inspecteur d'État de la Géorgie
- L'Institut national pour la transparence, l'accès à l'information et la protection des données personnelles, Mexique
- Le Centre national de la protection de la vie privée et des données, Moldavie
- Le Bureau de protection des données personnelles, Pologne
- Le Commissariat à l'information, Royaume-Uni
- L'Autorité de protection des données, Saint-Marin
- La Commission des données personnelles, Sénégal
- Le Préposé fédéral à la protection des données et à la transparence, Suisse

- Le Commissariat à l'information et à la protection de la vie privée, Terre-Neuve-et-Labrador
- L'Instance nationale de protection des données personnelles, Tunisie
- L'Agence des droits fondamentaux de l'Union européenne
- Le Contrôleur européen de la protection des données
- Le Commissariat victorien à l'information, Victoria

Nous aimerions également reconnaître la contribution cruciale des pairs évaluateurs externes et d'autres organismes de réglementation qui ont commenté le document, dont les suivants :

- La Commission canadienne des droits de la personne
- Le Conseil chilien de la transparence
- Le Conseil de l'Europe
- Le Bureau d'inspecteur d'État de la Géorgie
- L'Autorité de protection des données, Saint-Marin
- Le Commissariat à l'information et à la protection de la vie privée, Terre-Neuve-et-Labrador
- L'Agence des droits fondamentaux de l'Union européenne
- Le Contrôleur européen de la protection des données
- Le Commissariat victorien à l'information, Victoria
- Les membres du groupe de référence de l'Assemblée mondiale pour la protection de la vie privée**.**

Enfin, nous aimerions reconnaître les recherches, l'analyse et les efforts de rédaction précieux d'Orla Lynskey et de Judith Rauhofer, et les remercier, car ce présent rapport s'appuie sur leurs réflexions et leur synthèse.

1. Résumé

A. But de l'exposé

Au cours de la dernière décennie, de nombreux instruments internationaux importants de protection des données ont été modernisés, dont les Lignes directrices de l'Organisation de coopération et de développement économiques (OCDE) sur la protection de la vie privée, la Convention 108 du Conseil de l'Europe, et la réglementation en matière de protection des données de l'Union européenne (UE), alors que le nombre de lois sur la protection des données a augmenté à l'échelle nationale.[2]

Le présent exposé tient compte de ces faits nouveaux et appuie l'adoption d'une approche fondée sur les droits fondamentaux en ce qui concerne la protection des données et de la vie privée à l'échelle mondiale. Il répond à la question « que protégeons-nous lorsque nous protégeons la vie privée et assurons la protection des données? », en plus d'exprimer clairement le lien entre ces droits et d'autres droits et intérêts, comme la dignité humaine, la liberté et la liberté d'expression. Enfin, il énumère les obstacles potentiels à l'établissement de ces droits, en plus de suggérer des façons de les surmonter, ouvrant la voie au renforcement de ces droits dans les cadres juridiques nationaux et internationaux.

B. Liens avec l'initiative du Groupe de travail de l'AMVP

À la base de nos travaux, il y a l'idée que la protection de la vie privée et la protection des données sont des droits universels de la personne. Ces droits sont, eux-mêmes, fondamentaux pour notre démocratie, ainsi que l'exercice d'autres droits valorisés collectivement dans nos sociétés. Dans de nombreux contextes, ce sont nos droits à la vie privée et à la protection des données qui permettent l'exercice significatif d'autres droits fondamentaux, comme la liberté d'exprimer ses convictions politiques, la liberté de circulation et d'association, l'exercice des droits démocratiques, la dissidence pacifique et la liberté de conscience et d'expression[3].

Par exemple, au cours des cinq dernières années, le degré de vulnérabilité des procédures électorales face à l'intrusion et à la manipulation est devenu de plus en plus évident, illustrant que les problèmes d'ingérence étrangère, les protections en ligne et les droits à la vie privée et à la protection des données sont étroitement liés. Les gouvernements, les législateurs, les organismes de réglementation, les entreprises et la société civile doivent tous interagir les uns avec les autres pour relever ces défis complexes[4].

Sans égard aux motivations, il n'est plus possible de minimiser les risques complexes en matière de protection de la vie privée ou d'en faire abstraction. Certains font valoir que les institutions devraient en faire plus pour respecter les obligations juridiques fondamentales, tandis que d'autres veulent assurer la protection des droits individuels[5]. D'autres commentateurs soulignent les obligations organisationnelles quand vient le temps d'améliorer la reddition de comptes et la gouvernance, ou d'innover avec les données de manière plus transparente[6]. Chacun de ces points comporte ses critiques et ses défenseurs. Cependant, tandis que les

fins et motivations de différents intervenants demeurent fluides, le présent rapport montre que les mesures concrètes pour protéger la vie privée et les données sont désormais des obligations non négociables dans de nombreuses instances.

L'effort international déployé avait pour objectif de tenir compte de ces leçons et expériences de partout dans le monde, afin de mieux comprendre la mesure dans laquelle la protection significative de la vie privée est essentielle pour d'autres droits fondamentaux qu'il faut respecter et cultiver dans des sociétés ouvertes et libres[7].

C. Pourquoi cela importe-t-il?

Au cours de la dernière décennie, les percées technologiques, les nouvelles économies numériques, les réseaux de données mondialisés, la gouvernance axée sur les données, les nouveaux modèles opérationnels et les initiatives de gouvernement numérique d'une grande portée ont fait de la protection des libertés civiles un défi complexe et mondial.

Au cœur de ces changements, on trouve la collecte et le partage de données massives, le processus décisionnel automatisé et le profilage, autant par les organismes publics que les entités commerciales privées. Ces technologies et processus numériques et fondés sur les données ne font pas que soulever des préoccupations au sujet de la protection de la vie privée comme droit de la personne. Ils ont également des répercussions sur, entre autres, la dignité humaine, l'égalité, la non-discrimination et le droit à la réputation[8]. Il n'est pas exagéré d'affirmer que l'arrivée de nouvelles plateformes, pratiques et technologies numériques a eu et continuera d'avoir des effets historiques profonds sur les personnes et la société[9]. Ces effets seront comparables à ceux observés pendant la révolution industrielle ou au début de la période moderne, caractérisée par la prolifération de la presse à imprimer, ce qui a entraîné la Réforme, la Renaissance, la montée de l'État-nation et de nouvelles idées politiques, ainsi que des guerres et conflits associés à ces événements historiques.

Les outils numériques ont un potentiel tout aussi transformateur[10]. Tandis que notre société se trouve au début de cette transformation, nous voyons déjà la première génération d'enfants nés dans un monde où leur vie numérique fait partie de la réalité quotidienne. Il reste à savoir quelles seront les répercussions de la numérisation sur les personnes et la société, et comment nous pourrons veiller à ce que nos lois protègent nos valeurs et nos droits alors que la transformation numérique s'accélère[11].

2. Introduction : pourquoi cela importe-t-il maintenant?

En raison de la multiplicité des lois en matière de protection des données partout dans le monde et de l'engagement actuel en ce qui concerne la protection de la vie privée et des données comme droit fondamental dans de nombreux pays, on peut se demander, en toute légitimité : pourquoi cela importe-t-il maintenant? Le présent exposé préconise la reconnaissance du droit à la protection de la vie privée et du droit à la protection des données personnelles dans les États qui ne reconnaissent pas encore de tels droits. Dans le cas de ceux qui le font, l'exposé demande le renouvellement d'un engagement clairement défini en ce qui concerne ces droits et leurs principes sous-jacents. Une telle reconnaissance et une telle confirmation sont requises, de manière urgente, pour tenir compte d'importants changements technologiques et sociétaux.

Nos interactions quotidiennes sont de plus en plus numérisées. La technologie continue d'être appliquée de manière à faire progresser et à promouvoir nos droits fondamentaux dans certains cas, mais à les remettre en question dans d'autres[12]. Parmi les exemples judicieux de ce dernier point, il y a l'informatique affective, ou la technologie qui décèle les émotions. L'intelligence artificielle (IA) émotionnelle se sert des méthodes d'apprentissage machine pour vraisemblablement déduire l'état mental de ses sujets. Elle est utilisée à de vastes fins, allant de la surveillance de la sécurité routière des conducteurs à la publicité ciblée[13]. Une entreprise comme EyeQ, par exemple, offre une technologie de reconnaissance des émotions qui prétend fournir aux détaillants des données en temps réel sur les émotions et les données démographiques des clients (comme le genre et l'âge). Ces données peuvent « servir à améliorer le service et à accroître le taux de conservation[14] ».

De telles technologies peuvent exacerber l'asymétrie des pouvoirs et de l'information entre les entités qui recueillent et utilisent de telles données et les personnes dont les émotions sont ainsi évaluées. Tout particulièrement, cette technologie pourrait être utilisée de toute évidence pour exploiter les fragilités émotionnelles et les faiblesses cognitives. Même s'il peut être difficile de recueillir des preuves d'une telle exploitation, certaines indications laissent entendre que cette situation se produit déjà. En 2017, un organe de presse australien a indiqué que Facebook a vanté auprès des annonceurs sa capacité à pouvoir déterminer si les adolescents avaient « besoin d'un regain de confiance », s'ils se sentaient « instables » ou « inutiles »[15].

Lorsqu'on envisage la manière de réglementer de telles technologies, le postulat de départ de la législation fondée sur le marché, comme les lois de protection des consommateurs, qui se limitent à des ententes entre un « consommateur » et une « entreprise » et supposent que les personnes physiques agissent comme des agents rationnels lorsqu'ils prennent des décisions, comportera de toute évidence des lacunes[16]. C'est ici que la protection des données et le droit à la vie privée ont un rôle à jouer[17]. La technologie elle-même a changé en ce qui concerne la manière dont elle cherche à saisir et à représenter nos décisions et à influer sur notre comportement. Cependant, on observe aussi l'exercice de pressions croissantes sur le fait de tirer parti de ces avancées technologiques, sans tenir compte des conséquences élargies que cela pourrait avoir sur la société.

Dans le secteur privé, la philosophie « agissez vite et cassez les codes » mise en application par les jeunes entreprises de la Silicon Valley a favorisé la perception selon laquelle toute forme de réglementation, tout particulièrement la réglementation des droits fondamentaux, nuit à l'innovation, ainsi qu'à l'efficacité[18]. En galvaudant ainsi la protection des données et la réglementation de la vie privée, il devient plus facile de diffuser le mythe selon lequel, si l'on viole des droits fondamentaux tels que les droits à la vie privée ou à la protection des données, et si l'on accepte une nouvelle réalité dans laquelle le potentiel inexploité des données personnelles est débloqué, nous en sortons tous gagnants. Pourtant, comme le fait valoir le présent exposé, ce n'est qu'en intégrant les principes fondamentaux de protection des données et de protection de la vie privée que les technologies représenteront de véritables progrès de la société, qu'elles gagneront la confiance des personnes et des consommateurs, et que nos valeurs sociales, démocratiques et éthiques actuelles continueront d'être respectées.

Bien sûr, certaines écoles de pensée ne sont pas d'accord avec cette formulation. Pour accélérer l'innovation ou limiter la responsabilité juridique, par exemple, certains commentateurs soulignent l'importance de la responsabilité sociale des entreprises et des modèles de gouvernance, au lieu des obligations en matière de droits de la personne fondamentaux, quand vient le temps de tenir compte des préoccupations en matière de protection de la vie privée[19]. Depuis des décennies, l'industrie de la technologie avance des arguments semblables, tout en décourageant l'adoption de règlements restrictifs. À l'autre extrémité du débat, des chercheurs respectés mettent l'accent sur le pouvoir, les privilèges et la surveillance comme contrôle social, plutôt que sur les droits individualisés en matière de protection de la vie privée. Les deux groupes proposent des arguments légitimes[20]. Cependant, même si le profit et le pouvoir sont, de toute évidence, des facteurs légitimes, les organismes de réglementation considèrent plusieurs de ces termes (comme la responsabilisation vérifiable) et concepts (comme la surveillance indépendante) mis de l'avant par ces promoteurs comme étant complémentaires, non contradictoires.

Point opposé : vie privée, technologie et protection des droits

Ce ne sont pas tous les exemples de numérisation et de technologies de pointe qui ont érodé la vie privée. Il est important de souligner que certains progrès récents en ce qui concerne les technologies améliorant le respect de la vie privée ont favorisé considérablement la protection des droits de la personne. Certaines technologies, comme la vérification de l'identité à facteurs multiples (pour éviter les recherches d'appareil), les outils d'anonymisation (comme mesure pour lutter contre le blocage de contenu sur Internet) et le chiffrement de bout en bout (comme solution provisoire pour se soustraire à la surveillance gouvernementale), nous fournissent tous des exemples concrets illustrant comment des technologies numériques proposent désormais des protections très réelles et concrètes contre les risques relatifs à la vie privée. Parmi les exemples de telles technologies de chiffrement de bout en bout, il y a les réseaux privés virtuels. Par réseaux privés virtuels (RPV), on entend les technologies qui permettent aux utilisateurs d'accéder à Internet de manière sécurisée et privée. Les RPV peuvent chiffrer l'appareil de communication d'un utilisateur et réacheminer les données de réseau (habituellement une adresse IP) au moyen d'un mode sécurisé vers les serveurs étrangers du fournisseur de RPV, masquant ainsi l'adresse IP de l'utilisateur. Ainsi, les RPV peuvent permettre aux utilisateurs de se soustraire à la censure sur Internet et aux interruptions touchant les réseaux sociaux imposées par des gouvernements nationaux. Non seulement cette technologie préservant la vie privée permet aux utilisateurs d'accéder à des sites Web bloqués, mais elle leur permet également de coordonner, en toute sécurité, des mouvements sociaux et des manifestations politiques. Par exemple, en 2019, lorsque le gouvernement égyptien a bloqué l'accès aux sites des réseaux sociaux, comme Facebook et BBC News, afin de tenter de décourager les manifestations politiques, les Égyptiens ont été en mesure de contourner les interruptions touchant les réseaux sociaux au moyen de RPV. Ils ont pu ainsi continuer de coordonner les manifestations. Les RPV sont aussi fréquemment utilisés dans d'autres régions du monde, tout particulièrement dans les pays où les gouvernements ont imposé des restrictions visant Internet. L'utilisation et la popularité des RPV soulignent le lien entre le respect de la vie privée, la protection des données et les droits de la personne, car les RPV encouragent les gens à exercer leur droit de manifester, en plus de leur permettre de le faire.

Sources : *Surveillance et droits de l'homme : Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression (mai 2019); L. Gill, T. Israel, C. Parsons, Shining a Light on the Encryption Debate (2018); rapport « Ensuring Human Rights for Digital Citizens » (29-37) de la Global Commission on Internet Governance (juin 2016); Katherine Barnett, « The impact of social media on modern protest movements and democracy », The Sociable, 20 septembre 2019.* https://sociable.co/social-media/impact-social-media-modern-protest-movements-democracy/

La confiance et la transparence continuent d'être des thèmes récurrents dans tout ce genre de littérature, tout comme la question de savoir comment établir l'ordre de priorité des questions relatives à la technologie et comment les réglementer. Des gouvernements et des organismes du secteur public ont montré, d'une manière claire et persistante, qu'ils souhaitent s'attaquer aux enjeux sociétaux au moyen de solutions technologiques axées sur les données[21]. L'avantage associé au fait d'utiliser la technologie pour créer des solutions aux défis sociétaux, c'est son efficacité perçue (en ce qui concerne les coûts et le rendement), ainsi que la

capacité des solutions automatisées à faire l'objet d'audits et à être uniformes[22]. On pourrait ajouter la réticence des États à être à la traine en ce qui concerne la capacité de traitement des données, car cela nuirait à leur avantage concurrentiel sur la scène géopolitique compétitive en ce qui concerne l'IA à l'avenir[23].

Pendant la pandémie de COVID-19, ces solutions technologiques ont été le premier point de contact pour de nombreux organismes du secteur public. Parmi les exemples flagrants de cette situation, il y a le déploiement d'un algorithme pour calculer les résultats des examens scolaires finaux (niveau avancé) pour les élèves au Royaume-Uni. Le tollé soulevé par son déploiement a été tel que le premier ministre britannique l'a affublé du nom d'« algorithme mutant ». L'initiative a donc été abandonnée[24]. Alors que l'algorithme a été mis à exécution pour neutraliser les prédictions positives des enseignants au sujet du rendement de leurs élèves aux examens, en pratique, le modèle pénalisait les écoles qui avaient aidé les élèves à s'améliorer considérablement entre les examens ministériels, en les comparant au rendement scolaire moyen. Son exactitude a été contestée[25].

Comme le président de l'Open Data Institute l'a souligné, cet exemple a tout simplement mis en évidence les problèmes entourant le processus décisionnel automatisé lorsqu'il est déployé par le secteur public. Cependant, dans d'autres contextes délicats où il est utilisé, il est tout aussi percutant que les algorithmes du secteur privé, en n'attirant pas le même degré d'attention critique[26]. Le manque de transparence, avant et pendant le processus de déploiement, est amplifié par le fait qu'il n'y a plus de distinction entre l'utilisation publique et l'utilisation privée. Dans de nombreux cas, le secteur public comptera sur des outils créés, vendus et mis à l'essai par des entreprises sans étude minutieuse du processus d'approvisionnement. Ainsi, des outils sont mis en place avant qu'il y ait une discussion publique sur les objectifs et les répercussions.

Cet exemple a mis en lumière les inégalités sous-jacentes dans le système d'éducation, par exemple en favorisant systématiquement les élèves de cohortes plus petites par rapport à ceux de cohortes plus grandes, alors que les cohortes plus petites se trouvent habituellement dans les écoles privées. Cette situation confirme un danger évident associé à un tel solutionnisme technologique allant au-delà de la protection des données et du respect de la vie privée : les sociétés font de la technologie une solution par défaut pour résoudre quasiment tous les problèmes, de l'inégalité aux changements climatiques, au détriment des causes fondamentales de telles crises[27]. Tandis qu'il est impossible de faire abstraction de ces causes fondamentales, il ne faudrait pas non plus minimiser la capacité de la protection des données et du respect de la vie privée à accroître la confiance envers de tels systèmes. Au contraire, en intégrant les inégalités existantes aux solutions technologiques, on pourrait perpétuer ces défis, au lieu de s'attaquer à leurs causes.

Pendant la pandémie, la prestation de services numériques s'est accélérée dans les secteurs public et privé, tandis que les préoccupations concernant les droits ont souvent été mises de côté en raison de la crise mondiale[28]. Si elle ne fait pas l'objet d'une vérification, la croissance de cette forme de capitalisme axé sur la surveillance aura des répercussions profondes et durables sur de nombreux secteurs. En fait, elle pourrait réduire ou même renverser des attentes raisonnables antérieures en matière de protection de la vie privée dans certains domaines, comme le travail,

l’éducation et la médecine[29]. À la lumière de ces nouveautés technologiques et sociétales, il n’a jamais été aussi important pour les États d’affirmer ou de confirmer et d’énoncer de manière explicite, dans des lois écrites, leur engagement en matière de protection des données et de la vie privée.

Affirmer les droits, de manière explicite, dans les documents constitutionnels ou dans les lois, permet à tous les citoyens et à toutes les organisations de comprendre clairement qu’un droit est protégé et reconnu. Même si les États ont une jurisprudence qui confirme ou précise des droits, celle-ci relève du domaine des avocats et des universitaires. Il s’agit donc d’une affirmation plus opaque d’un droit. Dans la plupart des sociétés, le grand public n’est pas au courant, en général, des décisions juridiques. Il est donc mal placé pour soulever des préoccupations en ce qui concerne le non-respect de ses droits. Tandis que l’affirmation judiciaire est acceptable sur le plan juridique, elle ne permet pas tout le temps d’améliorer l’accès à la justice en pratique ni de protéger les droits en matière de vie privée.

En bref, il ne faut pas laisser cette protection à des organismes publics qui n’ont pas de comptes à rendre ou aux forces du marché. Cette protection est nécessaire, car elle agit comme contrôle essentiel sur le pouvoir croissant que les données et les infrastructures technologiques accordent aux acteurs publics et privés qui peuvent l’exercer sur nous, à titre de personnes physiques, sur les groupes et sur la société dans son ensemble. Notre but consiste à faire en sorte que les personnes physiques et les sociétés puissent continuer de tirer profit des services numériques, que ce soit pour socialiser, apprendre, magasiner ou interagir avec des services essentiels, d’une manière qui protège les données et respecte la vie privée, et qui respecte d’autres droits fondamentaux connexes. Les gens ont, après tout, le droit de vivre sans surveillance injustifiée de l’État et des entreprises.

3. Origines du droit à la protection de la vie privée et des données

Pour accroître le soutien international pour l'élaboration d'un mécanisme juridique international fondé sur les droits à la protection de la vie privée et à la protection des données, il est utile d'étudier tout d'abord la portée et l'histoire du droit général à la vie privée et du droit à la protection des renseignements personnels et des données.

A. L'origine du droit à la protection de la vie privée

Dans les nations occidentales développées et dans l'hémisphère nord de la planète, le droit à la protection de la vie privée a suivi une trajectoire particulière comme droit de la personne universel. En ce qui concerne la compréhension culturelle originale, les gens associent souvent l'idée de la protection de la vie privée à une dimension physique ou à un endroit, comme le foyer, alors que le niveau de protection dépend du degré auquel ce lieu est ou devrait être accessible aux autres. Dans un contexte moins concret, on considère souvent la protection de la vie privée comme une forme de secret (par cela, on entend que le respect de la vie privée prend fin lorsque le secret est partagé) ou de confidentialité (selon laquelle une ingérence est une violation de la confiance mutuelle). Cette situation a été démontrée il y a quelque deux mille ans, lorsque Cicéron a rédigé son *Traité des devoirs*, prenant la forme de conseils à son fils, qui envisageait une carrière au sein de la fonction publique de l'État romain[30]. Cicéron a demandé au membre plus jeune de la famille de réfléchir à ce que les citoyens attendent du gouvernement, de réfléchir aux résultats qu'un gouvernement doit finalement obtenir. Quelles sont nos attentes envers lui?

Cicéron est passé de procureur public à consul de Rome, posant de telles questions à son gouvernement. Pourquoi la loi romaine insistait-elle sur le fait de faire une distinction si évidente entre les aspects privés et l'espace privé et les aspects gouvernementaux et la propriété publique? Il a conclu que tout gouvernement adéquat doit protéger le caractère sacré des sphères publique et privée. Ce raisonnement résiste à l'épreuve du temps. Pourquoi avons-nous un gouvernement et des lois si ce n'est pas pour définir la limite entre la vie personnelle des citoyens et les objectifs de l'État?

Ainsi, selon le droit romain antique, le pouvoir du gouvernement de s'introduire dans la propriété privée, de fouiller l'espace privé et de saisir des documents ou des biens privés, doit être considérablement limité par la loi si l'on veut protéger la vie privée d'une manière significative[31]. De telles limites et restrictions imposées à l'immixtion et à la coercition de l'État dans le domaine privé font en sorte que la vie privée relève carrément des mécanismes intellectuels à l'appui de l'application courante de la loi et de la primauté du droit.

L'autre similitude entre le droit à la vie privée (tout particulièrement en ce qui concerne les communications) et la primauté du droit (plus précisément, les exigences en matière d'application courante de la loi), il y a le fait qu'il s'agit de réactions de base particulières au problème que représentent les pouvoirs d'État intrusifs[32]. Si on évalue un aspect encore plus précis du débat sur la protection de la vie privée dans le domaine juridique, comme le caractère confidentiel des documents et des communications personnels, on observe encore d'autres échos

datant d'époques lointaines. Plus particulièrement, en 1215, lorsque le roi Jean a signé la *Grande Charte*, celle-ci protégeait le droit personnel contre toute saisie illégale du gouvernement et tout accès illégal aux biens personnels d'une personne. Plus précisément, on peut lire, à la 39e disposition de la *Grande Charte* :

> [traduction]
>
> *« Aucun homme libre ne sera saisi, ni emprisonné ou dépossédé de ses biens, déclaré hors-la-loi, exilé ou exécuté, de quelque manière que ce soit. Nous ne le condamnerons pas non plus à l'emprisonnement sans un jugement légal de ses pairs, conforme aux lois du pays. »*

La *Grande Charte* constituait une réaction sur le plan de la primauté du droit aux mandats intrusifs de la Couronne, tout comme le quatrième amendement de la *Constitution américaine*[33]. À la base, la primauté du droit établit un ensemble de conditions à respecter avant que le gouvernement puisse prendre des mesures intrusives ou coercitives. Autrement dit, le gouvernement ne peut arrêter une personne, fouiller ou saisir ses possessions, ses biens et ses documents dans le cadre d'un processus légal autorisé par un juge (jugement légitime) ou le parlement (lois du pays)[34]. À la suite de l'injonction datant de 800 ans de la *Grande Charte* sont apparus les débats sur les mandats, l'application courante de la loi de base et les pouvoirs de fouille et de saisie du gouvernement[35]. Ces préoccupations sont maintenues, allant de la réflexion de James Madison et d'Alexander Hamilton dans leurs *Federalist Papers* à la jurisprudence fondée sur les principes énoncés par Warren et Brandeis[36].

Même si l'évolution du droit à la protection de la vie privée des personnes physiques a pris du temps (avant le XVIIe siècle), il y avait une distinction de longue date dans le terme latin *privatus*, entre les questions qui relèvent du domaine collectif (et qui relèvent donc du pouvoir public) et les questions qui relèvent d'une communauté close (qui relèvent d'un ménage)[37]. Diane Shaw a écrit que [traduction] « la thèse erronée selon laquelle la notion de la sphère intime était absente dans la société médiévale découle possiblement de l'hypothèse moderne selon laquelle la vie privée est individuelle et absolue, au lieu d'être commune et relative »[38]. Comme l'indique de manière succincte David Vincent, le discours sur la vie privée ne représente pas une progression allant de l'absence à l'invention, ni nécessairement de moins à plus. Il s'agit plutôt d'un droit fondamental qui a toujours été à la base de notre compréhension de la vie individuelle et collective, [traduction] « alors qu'il n'y a aucun commencement à cette histoire, seulement des fins menacées »[39].

Ces fondements historiques occidentaux de la vie privée et le fait qu'on considère cette dernière comme une forme de secret, c'est-à-dire que la vie privée cesse d'exister lorsque le secret est partagé, ou de confidentialité, selon laquelle une intrusion est définie comme une violation de la confiance mutuelle, ont été peu remis en question avant la fin du XIXe siècle, lorsque Samuel Warren et Louis Brandeis ont rédigé leur essai de 1890, s'intitulant *The Right to Privacy*. Selon Warren et Brandeis, la protection de la vie privée équivaut au [traduction] « droit d'être laissé tranquille », mettant en doute la conceptualisation classique[40].

Plus particulièrement, l'essai cherchait à déterminer des éléments fondamentaux du droit pour offrir un droit plus actif aux personnes physiques quand vient le temps de contrôler la divulgation de leurs « réflexions, sentiments et émotions » et empêcher cette divulgation de la même manière qu'ils peuvent déjà interdire à d'autres personnes de pénétrer dans un lieu physique qui relève d'eux (au moyen de la règle relative à l'immixtion)[41]. Allant au-delà de certaines notions, comme « lieu », « secret » ou « confidentialité », cette approche nouvelle repose notamment sur l'élargissement de la sphère de protection de la vie privée. Au lieu de restreindre le droit à une dimension purement spatiale, elle comprend, entre autres, le droit de la personne de contrôler les renseignements à son sujet.

Cette notion de la vie privée comme droit individuel en ce qui concerne le contrôle de l'information a été maintenue au XX^{e} siècle, alors que la montée de régimes autoritaires et totalitaires à travers le monde a décuplé les efforts déployés pour établir un droit à la vie privée. Parmi les questions en jeu, il y avait la capacité de ces régimes à exercer des pouvoirs sur leurs citoyens en raison d'un accès à des renseignements détaillés sur l'identité, les réflexions, les croyances et les actions de ces citoyens, et de la possibilité d'influer sur leur comportement et de le contrôler en conséquence.

À la suite de la Deuxième Guerre mondiale, cette expérience a fait en sorte que les gouvernements démocratiques ont reconnu, en grande partie, que le respect de la vie privée devait être un droit de la personne reconnu afin de maintenir la démocratie. Cela permettait de protéger les personnes physiques de l'immixtion dans leur vie privée et familiale, tout particulièrement, mais pas exclusivement, par les acteurs gouvernementaux. Il faut préciser que nous reconnaissons pleinement qu'il s'agit de points particuliers de la pensée libérale classique. Dans certains cas, le discours mondial sur le respect de la vie privée a été façonné par cet ensemble particulier d'expériences historiques. Cependant, cela ne devrait pas permettre de dissiper les préoccupations. On devrait faire la promotion du respect de la vie privée et de la protection des données comme droits universels, au moyen de mécanismes internationaux, tout particulièrement parce que ces risques autrefois particuliers sont devenus universels en raison de la libre circulation des données, des nouvelles technologies, des modèles opérationnels internationaux et de l'harmonisation des pratiques gouvernementales.

i. Le droit à la vie privée à l'échelle internationale

À l'échelle internationale, la *Déclaration américaine des droits et devoirs de l'homme* (ADRDM) a été le premier document à énumérer des droits. Elle a été adoptée par les nations des Amériques en mai 1948. Au cours de la même année, les Nations Unies (ONU) ont promulgué la *Déclaration universelle des droits de l'homme* (DUDH), qui prévoit de vastes protections de la vie privée. Selon l'article 12 de la DUDH :

> *Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.*

En mettant en valeur un vaste concept général de vie privée, l'ADRDM et la DUDH ont ouvert la voie à des conceptions plus élargies de la vie privée, allant au-delà de la vie privée dans certains lieux, comme le foyer, ou contextes, comme la vie familiale. Des mécanismes internationaux subséquents ont suivi cette tendance en ce qui concerne la protection de la vie privée élargie. Par exemple, sur le planrégional, l'Organisation des États Américains (OEA) reconnaissait à toute personne, dans la Convention américaine relative aux droits de l'homme, le « droit au respect de son honneur et à la reconnaissance de sa dignité. Nul ne peut être l'objet d'ingérences arbitraires ou abusives dans sa vie privée, dans la vie de sa famille, dans son domicile ou sa correspondance, ni d'attaques illégales à son honneur et à sa réputation ».

La *Convention européenne des droits de l'homme* (CEDH), adoptée par le Conseil de l'Europe en 1950, et entrée en vigueur en 1953, était le premier mécanisme international contraignant à reconnaître un droit général en matière de protection de la vie privée. Le paragraphe 8(1) définit le droit (« toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance ») avant de déterminer les conditions visant à limiter ce droit à l'article 8(2) de la CEDH.

Ensuite, l'ONU a adopté le *Pacte international relatif aux droits civils et politiques* (PIDCP), ainsi qu'un protocole facultatif connexe en 1966[42]. Les États membres de l'ONU ont été invités à signer et ratifier ces documents additionnels, qui étaient contraignants pour ceux les ayant ratifiés. Le droit à la vie privée est énoncé à l'article 17 du PIDCP, qui prévoit ce qui suit :

1. *Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation.*
2. *Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.*

Afin de surveiller la conformité, le Conseil des droits de l'homme (CDH) des Nations Unies tient compte de rapports périodiques (présentés par les États membres du PIDCP) sur le respect des droits en vertu du PIDCP[43]. Jusqu'à maintenant, le CDH a diffusé plus de 100 opinions sur le respect de l'article 17 du PIDCP par les États membres[44]. Cependant, le statut légal de ses conclusions ou « opinions » continue d'être contesté[45]. En 2015, un Rapporteur spécial sur le droit à la vie privée de l'ONU a été désigné. Il est chargé de faire des recherches et de publier des rapports sur un vaste éventail de questions en matière de protection des données et des droits numériques[46].

La Charte de l'ONU a mandaté un autre organisme, la Commission du droit international, pour mener des études et formuler des recommandations pour inciter à « l'élaboration progressive du droit international et de sa codification »[47]. La « protection des données personnelles lors des transferts transfrontaliers de renseignements » a été ajoutée au programme de travail à long terme de la Commission du droit international en 1997. Ces travaux ont avancé en raison, entre autres, des travaux stratégiques et des rapports de différents rapporteurs spéciaux pertinents, comme ceux chargés de la liberté d'opinion et d'expression, du droit à la

vie privée et des droits des enfants. De plus, les activités internationales de défense des intérêts des titulaires de droits individuels et des organisations nationales de droits de la personne continuent de servir à l'élaboration et à l'interprétation des mécanismes de droits modernes et d'examens au sein de l'ONU, en plus d'influer sur ceux-ci. Ces efforts ont permis de réaliser des progrès évidents (comme la DNUDPA), et joueront probablement un rôle essentiel lors de l'élaboration future de nouveaux mécanismes en matière de protection de la vie privée.

ii. Le droit à la vie privée à l'échelle nationale

À l'échelle nationale, le droit à la protection de la vie privée ou des données a été établi, de manière courante, de l'une des quatre manières suivantes :

Dispositions constitutionnelles : Tout d'abord, les pays peuvent ajouter formellement des droits à la protection de la vie privée parmi les droits fondamentaux prévus dans leurs constitutions nationales ou déclarations des droits[48]. Bien que rare jusque dans les années 1960 et 1970, cette approche est désormais mise en application par, entre autres, le Mexique, la Suisse, la Belgique, la Corée, les Philippines, Hong Kong, le Portugal, la Colombie, le Chili, Trinité-et-Tobago et le Gabon. Parmi ces derniers, plusieurs ont ensuite intégré ces droits à leur constitution actuelle[49]. Ce ne sont pas tous ces pays qui reconnaissent un droit général à la protection de la vie privée. Cependant, leurs constitutions peuvent comprendre des droits qui protègent un aspect particulier de la vie privée. Par exemple, la Constitution des Bermudes protège un droit très précis à la protection de la vie privée du foyer d'une personne et d'autres biens[50]. Dans des pays dotés d'une structure fédérale, les droits à la vie privée ou à la protection des données peuvent aussi être ajoutés aux constitutions pertinentes des États, au lieu de la constitution fédérale. Par exemple, en Allemagne, les constitutions des « *Neue Bundesländer* » (les États qui ont été intégrés à la République fédérale à la suite de la réunification de l'Allemagne de l'Ouest et de l'Allemagne de l'Est en 1990) et de nombreux autres États comprennent un droit exprès à la protection de la vie privée et des dispositions concernant l'autodétermination en ce qui concerne les renseignements, la confidentialité des renseignements ou la protection des données[51]. Dans le même ordre d'idées, l'État de Victoria, en Australie, a intégré le droit à la protection de la vie privée à l'article 13 de la charte victorienne des droits de la personne et des responsabilités de 2006.

Législation particulière : Faisant l'objet de discussions détaillées dans la section suivante sur l'origine du droit à la protection des données, de nombreuses instances ont créé, pendant les années 1960 et 1970, des lois en matière de protection de la vie privée ou des données propres à des secteurs. Certains États peuvent même reconnaître de manière officielle le droit dans une loi quasi constitutionnelle, comme des codes nationaux en matière de droits de la personne ou des lois sur la protection de la vie privée.

Jurisprudence : Dans les pays dont la constitution ne comprend pas, de manière expresse, des droits à la protection de la vie privée ou à la protection des données, les tribunaux nationaux peuvent, malgré tout, établir de tels droits par renvoi à un autre droit ou se fonder sur un ensemble d'autres droits. Par exemple, le tribunal

constitutionnel de l'Allemagne reconnaît un droit général à la personnalité, ainsi qu'un droit à l'autodétermination concernant les renseignements en vertu de l'article 2(1) (droit à l'autodétermination) et de l'article 1(1) (droit à la dignité) de la Loi fondamentale allemande[52]. Dans le cadre des droits à la liberté, le Canada protège certains aspects de la vie privée des personnes physiques des fouilles et saisies déraisonnables, comme l'indiquent les articles 7 et 8 de la *Charte canadienne des droits et libertés*[53]. Une approche semblable a été adoptée par les États-Unis, protégeant les « attentes raisonnables en matière de respect de la vie privée » des personnes physiques dans le cadre des quatrième et quatorzième amendements (protection contre les fouilles et saisies déraisonnables et application courante de la loi). Au Japon, l'article 13 de la Constitution (droit à la poursuite du bonheur) a été interprété par les tribunaux d'une manière y intégrant le droit à la vie privée[54]. Plus récemment, en 2017, la Cour suprême de l'Inde a déclaré que le respect de la vie privée fait partie des droits fondamentaux, puisqu'il s'agit d'un aspect intégral du droit à la vie et à la liberté personnelle garanti par l'article 21 de la Constitution de l'Inde. La décision positionnait la vie privée parmi la gamme complète de droits fondamentaux énumérés par la Constitution, et soulignait la manière dont elle permettait l'exercice d'autres droits, comme la liberté de parole et d'expression, la liberté d'association, la liberté de religion et le droit à l'égalité[55].

Accords et traités internationaux : Par ailleurs, des pays peuvent décider de mettre directement en application, à l'échelle nationale, des mécanismes internationaux de droits de la personne auxquels ils participent. Ils peuvent également adopter ces mécanismes internationaux comme loi nationale contraignante d'une manière qui permet leur application par les tribunaux nationaux. Par exemple, les 55 pays membres de la Convention 108 ont adopté des lois qui respectent les dispositions de la Convention. La Charte des droits fondamentaux de l'UE s'applique directement dans les 27 États membres de l'UE lorsqu'ils adoptent ou appliquent une loi nationale mettant en œuvre une directive de l'UE ou lorsque leurs autorités appliquent directement un règlement de l'UE[56]. En 1964, l'Autriche a accordé, de manière rétrospective, le statut constitutionnel national à la CEDH, alors que le Royaume-Uni, après avoir été l'un des premiers signataires (et rédacteurs) de la Convention, a finalement décidé de la rendre contraignante et de permettre son application par les tribunaux britanniques en 1998[57]. Une approche semblable a été adoptée par l'île de Man, une colonie de la Couronne britannique, lorsqu'elle a adopté sa Loi sur les droits de l'homme en 2001.

B. L'origine du droit à la protection des données

Contrairement au droit à la vie privée, présenté d'une manière assurément descendante dans le cadre de mécanismes de droits fondamentaux en grande partie internationaux, on pourrait faire valoir que le droit à la protection des données a été élaboré plutôt d'une manière ascendante. On décrit souvent son émergence comme une réponse aux progrès technologiques et à l'élaboration de nouveaux modèles opérationnels utilisant beaucoup de données, découlant du souhait de protéger les personnes physiques de leurs effets potentiellement négatifs. Ces effets comprennent, plus précisément, la collecte, l'utilisation, le stockage, le regroupement, le partage et la divulgation non autorisés des données personnelles d'une personne.

L'État allemand d'Hesse montre des traces de l'origine contemporaine des cadres modernes des lois sur la protection des données. Il est reconnu pour avoir adopté le premier mécanisme législatif de protection des données, soit la loi de protection des données d'Hesse de 1970[58]. Même si l'État a été, sans aucun doute, le premier à adopter une loi de ce genre, il a été rapidement suivi par un certain nombre d'autres pays, principalement européens, y compris, en 1977, la République fédérale d'Allemagne[59]. À l'époque, aucun droit à la protection des données n'avait été expressément ajouté à la Constitution de l'Allemagne, aux constitutions des « Länder » allemands ni aux constitutions des pays européens[60].

S'inspirant de ces changements et conscients de la circulation transfrontalière accrue des données personnelles, des experts internationaux ont rédigé l'ébauche de deux documents internationaux à la fin des années 1970, les *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* de l'OCDE, ainsi que la Convention 108. Cette dernière était un mécanisme multilatéral ouvert qui se fondait sur la Convention de Vienne sur le droit des traités, qui a ouvert la voie à l'adoption de futures lois nationales et régionales en matière de protection des données, y compris la Directive 95/46/CE de l'UE. La Convention 108 a été le premier mécanisme multilatéral contraignant en matière de protection des données, jetant les bases de la législation moderne dans ce domaine, en exigeant que les États membres appliquent les principes généraux de la protection des données (comme le traitement juste et légal des données, les fins précisées et légitimes, la qualité des données et un régime de circulation transfrontalière des données). Le tout est rapidement devenu influent, tout d'abord parmi les États membres du Conseil de l'Europe et, dès 2013, sur d'autres continents. L'Union européenne, perçue comme le chef de file mondial en matière de protection des données et disposant d'une structure de gouvernance régionale/nationale/étatique quasi fédérée, est un exemple utile quand vient le temps d'examiner ce « mythe de création ».

L'UE a utilisé expressément le terme « loi secondaire »[61] pour renvoyer à la Convention 108 lors de l'adoption de son cadre exhaustif de protection des données, indiquant qu'elle avait pour objectif de donner une portée aux principes énoncés dans la Convention 108, en plus de les amplifier[62]. La Directive 95/46/CE sur la protection des personnes en ce qui concerne le traitement des données personnelles et la libre circulation de ces données (« Directive de 1995 ») a été adoptée en 1995 à titre de mécanisme de marché commun dans le but d'harmoniser les cadres nationaux de protection des données des États membres de l'UE qui avaient été créés au cours des deux décennies précédentes[63]. La Directive de 1995 voulait fournir une norme de base en matière de protection parmi les États membres, en cherchant à assurer « la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel » et en facilitant la libre circulation des données personnelles entre les États membres, conformément aux objectifs de la Convention 108[64].

À l'époque, l'UE n'avait pas encore adopté son propre cadre de droits fondamentaux. Elle comptait principalement sur une compréhension commune, par les États membres, du fait que la définition des « droits fondamentaux » mentionnés

à l'article 1 de la Directive comprenait les dispositions de la CEDH du Conseil de l'Europe (que tous les États membres avaient ratifiée), ainsi que les droits fondamentaux protégés par les constitutions nationales ou déclarations des droits propres aux États membres. L'absence d'un cadre général sur les droits fondamentaux n'a donc pas empêché l'UE d'adopter un cadre exhaustif de protection des données se fondant, en grande partie, sur la Convention 108. La Charte des droits fondamentaux de l'Union européenne, qui comprend désormais un droit exprès à la protection des données à l'article 8, a été adoptée dans le cadre du Traité de Lisbonne. Elle est entrée en vigueur le 1er décembre 2009[65]. Ce lien très étroit, qui pourrait même être une symbiose, se fondant sur des principes et valeurs communs aux deux cadres de protection des données a été de nouveau mis en valeur lorsque les deux cadres ont été mis à jour dans une déclaration de la Commission de l'UE signalant que l'UE se joindrait à la Convention 108+ au moment de son entrée en vigueur[66].

Dans le contexte des Nations Unies, le seul mécanisme de l'ONU qui vise précisément la protection des données est constitué d'un ensemble de « Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel » non contraignant datant de 1990[67]. Comme Kuner le souligne, même si la base normative de la loi en matière de protection des données se fonde grandement sur les textes concernant les droits internationaux de la personne, comme la DUDH de 1948 et le PIDCP de 1966, ces mécanismes ne mentionnent pas, de manière précise, la protection des données[68]. C'est pourquoi, même si le droit à la protection des données est reconnu explicitement dans certaines constitutions nationales, la Charte des droits fondamentaux de l'UE est le seul mécanisme international existant qui reconnaît la protection des données comme un droit fondamental distinct[69]. L'UE a revu et mis à niveau son cadre de protection des données en 2016, en adoptant le Règlement général sur la protection des données (RGPD) et la Directive sur la police. Les deux lois continuent de rester ancrées dans les principes établis par la Convention 108.

i. Efforts modernes pour renforcer les droits à la protection des données et à la protection de la vie privée à l'échelle internationale

Nous pouvons constater que, même si la protection de la vie privée et la protection des données sont reconnues à grande échelle dans les pays aux quatre coins du monde et dans le contexte de différents arrangements constitutionnels, elles continuent d'être peu définies et sous-utilisées à l'échelle internationale. Le droit à la protection des données n'est toujours pas un droit reconnu à l'échelle internationale. Il n'est donc pas surprenant que certains exigent que ces droits soient davantage reconnus et appliqués à l'échelle internationale.

La Déclaration de Montreux de 2005, préparée lors de la Conférence internationale des Commissaires à la protection des renseignements personnels et de la vie privée (CICPRPVP), désignée maintenant par le nom Assemblée mondiale de la protection de la vie privée (AMVP)[70], constitue un exemple éloquent de cet appel au renforcement de ces droits. Par l'intermédiaire de la Déclaration de Montreux, la CICPRPVP a souligné « qu'il est nécessaire de renforcer le caractère universel de ce droit [à la protection des données et de la vie privée] afin d'obtenir une

reconnaissance universelle des principes régissant le traitement de données à caractère personnel tout en respectant les diversités juridiques, politiques, économiques et culturelles[71] ». La Déclaration demandait à l'ONU de préparer un mécanisme contraignant, « énonçant en détail le droit à la protection des données et de respect de la vie privée en tant que droits de l'homme exécutoires[72] ». La Résolution de Madrid de la CICPRPVP sur les normes internationales de protection des données personnelles et de la vie privée représentait un appel semblable, lancé en novembre 2009[73]. Des tentatives subséquentes ont été faites par l'intermédiaire de la CICPRPVP/l'AMVP, afin de préparer l'ébauche d'un mécanisme juridique mondial sur la protection des données en 2009, et de défendre l'adoption d'un troisième protocole facultatif du PIDCP en vue de l'adoption d'une norme internationale en matière de protection de la vie privée allant de pair avec l'article 17 du PIDCP[74].

Ces efforts pour renforcer les droits à la protection des données et à la protection de la vie privée à l'échelle internationale ne sont pas terminés. Cette situation peut être attribuable à l'inefficacité des mécanismes d'application de la loi actuels et des perspectives divergentes des différents États. Parmi les autres facteurs contribuant à la situation, il peut y avoir un déséquilibre dans la répartition de l'information et du pouvoir dans les environnements numériques modernes. De plus, les priorités en matière de réglementation touchent un vaste éventail de secteurs, d'enjeux et d'intervenants. Les deux phénomènes empêchent de percevoir facilement les risques en matière de protection de la vie privée ou d'exercer les droits avec efficacité. Malgré tout, la voie en matière de coopération internationale se précise.

Tout d'abord, la coopération internationale actuelle dans ces domaines a eu un succès limité[75]. Cela est attribuable à un certain nombre de facteurs. Certains sont associés aux caractéristiques des mécanismes de l'ONU, constitués d'un éventail de règles propres à différents mécanismes. Cette dispersion normative a des répercussions sur leur accessibilité et leur efficacité. De plus, en raison de leur nature caractérisée par le droit souple, plusieurs de ces mécanismes existants, comme les Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel, ne sont pas invoqués ni mis en application par le CDP[76]. Selon certains, cette absence d'utilité pratique est attribuable au moment, alors que les principes directeurs pertinents de l'ONU ont été adoptés après l'adoption d'importants mécanismes internationaux, comme les Lignes directrices sur la protection de la vie privée de l'OCDE et la Convention 108 du Conseil de l'Europe[77]. Pourtant, même dans le cas des régimes de protection de données qui sont considérés comme des exemples de réussite sur le plan des droits fondamentaux, comme le RGPD de l'UE, il demeure un décalage entre la lettre de la loi et son application pratique[78].

Pourtant, même s'il faut en faire plus pour promouvoir et appliquer les cadres internationaux et régionaux existants en matière de protection des données, il serait erroné de conclure que ces cadres n'ont aucune incidence. La Cour interaméricaine des droits de l'homme a créé un ensemble important de jurisprudence établissant une vision à facettes multiples pour le droit à la vie privée, en plus d'imposer une obligation positive aux États quand vient le temps de garantir le respect de ce droit par les entités publiques et privées, ainsi que les personnes physiques[79]. Les dispositions d'accords internationaux, dont les mécanismes de l'ONU, sont aussi

souvent reconnues, sur le plan constitutionnel, par les constitutions nationales. Par exemple, la Loi fondamentale de la zone administrative spéciale (ZAS) qu'est Hong Kong accorde un effet constitutionnel aux dispositions du PIDCP. Les mécanismes régionaux de droits de la personne qui reconnaissent des droits à la protection des données et à la protection de la vie privée, comme la Charte des droits fondamentaux de l'UE, ont également été invoqués d'une manière considérable pour remettre en question et finalement invalider des mécanismes législatifs incompatibles[80]. Finalement, même s'il reste difficile d'améliorer l'efficacité de ces cadres juridiques supranationaux, les efforts déployés ont déjà des répercussions concrètes. Il vaut la peine de continuer à les déployer.

Des perspectives divergentes ont également limité la reconnaissance de la protection des données et du respect de la vie privée comme droits[81]. Aujourd'hui, il n'est pas aussi facile de diviser les opinions sur cette question en fonction de frontières géographiques. De nombreux représentants commerciaux et autres intervenants craignent qu'un engagement constant et fort en ce qui concerne la protection des droits fondamentaux exige de futurs développements technologiques et commerciaux. Ce point de vue prévaut, malgré la croissance rapide et une hausse de la marge de profit dans les secteurs technologiques. D'autres considèrent, à tort, que le respect de la vie privée est un « obstacle » ou une « entrave » à l'innovation. Ils peuvent sinon reconnaître les aspects commerciaux et d'affaires de l'innovation, tout en faisant fi de la nécessité tout aussi urgente de soutenir l'évolution sociale et juridique.

Cette perspective explique, en grande partie, pourquoi [traduction] « lorsqu'on fait fi du niveau le plus élevé d'abstraction, il peut y avoir des différences considérables en ce qui concerne les détails » des approches régionales et nationales en matière de protection des données[82].

Différences : liberté d'expression au Royaume-Uni

Parmi les autres points qui différencient les États, on trouve leur position sur la liberté d'expression. De manière générale, dans les États où il y a une grande tradition en matière de liberté d'expression sur le plan juridique, on constate une réticence à reconnaître ou définir pleinement le droit à la protection de la vie privée. En Angleterre et au Pays de Galles, les tribunaux ont refusé de définir un droit à la protection de la vie privée sans fondements législatifs. Aussi récemment que les années 1990, la Cour d'appel a déclaré, de manière formelle, « qu'il est bien connu que, dans la loi anglaise, il n'y a aucun droit à la vie privée. En conséquence, il n'existe pas de droit d'action en cas de violation de la vie privée d'une personne ». Cependant, cet exemple illustre aussi que, si un droit à la vie privée est reconnu par un système juridique national, comme cela a été le cas au Royaume-Uni sous l'empire de la Loi sur les droits de l'homme de 1988 et finalement par la Chambre des lords dans le jugement Campbell de 2004, il peut s'intégrer rapidement et devenir un aspect bien établi du paysage juridique. Il est donc possible de surmonter ces obstacles culturels et idéologiques à la coopération, ce qui permet de faire preuve d'optimisme au sujet de la portée quand vient le temps de définir les droits à la protection de la vie privée et des données à l'échelle internationale. **Sources :** *Kaye v. Robertson* [1991] FSR 62, le juge Glidewell; *Campbell v. Mirror News Group* (MGN) [2004] UKHL 22.

Nous pouvons établir une différence entre deux approches en ce qui concerne l'élaboration et la mise en application de mécanismes régionaux en matière de protection des données et de la vie privée. La première se fonde principalement sur la reconnaissance des répercussions du traitement des données personnelles sur les *droits fondamentaux* (comme la *Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel*, la Convention 108 et le RGPD). La deuxième approche considère les *données comme un bien essentiel*, un actif commercial ou un intrant pour les biens et services. Elle cherche donc à maximiser son potentiel en ce qui concerne les échanges et le commerce, en minimisant la friction réglementaire (comme les Lignes directrices sur la protection de la vie privée de l'OCDE et le Cadre de protection de la vie privée de l'APEC). En pratique, ces régimes affichent cinq différences considérables.

Tout d'abord, l'interprétation des cadres fondés sur les droits est orientée par le raisonnement relatif aux droits fondamentaux (y compris, par exemple, l'intégration des évaluations de la nécessité et la proportionnalité). En revanche, les approches fondées sur le marché intègrent des hypothèses fondées sur le marché (comme le paradigme « de notification et de choix »). Ensuite, les cadres fondés sur les droits accordent des droits aux personnes physiques (les titulaires de droits), comme un droit d'accès, un droit d'obtenir la suppression des renseignements personnels et un droit de refuser le traitement des données. Ces droits sont associés à des obligations corrélées auxquelles les États et les entités privées (détenteurs d'obligation) doivent se conformer, afin de respecter ces droits. De tels droits sont absents des régimes axés sur le marché ou ont une importance moindre. Ensuite, les régimes fondés sur les droits reçoivent souvent l'appui de lois et de mécanismes d'application de la loi contraignants mis en application par une autorité indépendante en fonction d'aspects relatifs au droit public.

Ce système fondé sur les droits reconnaît que toute violation des droits individuels nuit au bien collectif, et qu'il est dans l'intérêt public de protéger, d'appliquer et de promouvoir ces droits en tenant responsables les entités qui ne les respectent pas. Alors que dans le cas des approches fondées sur le marché, la reddition de comptes prend plus souvent la forme de mesures relevant du droit privé, comme la résolution de différends commerciaux ou des poursuites en fonction de la jurisprudence en matière de contrats ou de délits. Enfin, une approche fondée sur les droits reconnaît le droit inhérent à la dignité des citoyens, et tient compte, de manière explicite, des déséquilibres de pouvoir pour protéger les personnes moins puissantes contre tout préjudice, alors qu'une approche fondée sur le marché privé fait souvent fi de tels déséquilibres et suppose que les préjudices seront automatiquement calculés lors de l'établissement du coût d'un bien ou d'un service au moyen des forces du marché.

Malgré tout, il reste qu'une convergence entre ces logiques apparemment distinctes est possible. Le respect de la protection des données et de la vie privée est souvent une condition juridique préalable pour la libéralisation de la circulation des données personnelles, brouillant les limites entre les approches fondées sur le marché et celles fondées sur les droits. De plus, le respect de ces droits est aussi une condition préalable pour assurer la confiance des utilisateurs en ce qui concerne l'utilisation des données à des fins novatrices. C'est pourquoi, tout comme le fait de promouvoir

le respect des principes environnementaux aide à assurer la durabilité à long terme, la promotion du respect de la protection des données et de la vie privée peut aider à garantir une innovation durable.

C. En quoi la protection des données consiste-t-elle? En quoi diffère-t-elle de la protection de la vie privée?

Comme nous l'avons mentionné précédemment, par rapport au droit à la vie privée, l'origine de la protection des données comme droit et son caractère fondamental précis sont un peu plus récents[83]. Depuis que le droit à la protection des données a été intégré pour la première fois aux constitutions nationales au cours des années 1970 et 1980, les tribunaux et les universitaires ont eu de la difficulté à tracer des lignes de démarcation évidentes entre les deux droits. Cette situation est compliquée par le fait que, même si un droit à la protection des données figure désormais dans un nombre croissant de constitutions de pays et d'États, la Charte de l'UE est, jusqu'à maintenant, le seul mécanisme juridique international qui fait une distinction explicite entre le droit à la protection des données et le droit à la protection de la vie privée[84].

Les mécanismes juridiques nationaux et internationaux qui prévoient expressément un droit à la protection des données ont un certain nombre de caractéristiques en commun[85]. Plus particulièrement, les mécanismes juridiques nationaux et internationaux qui protègent précisément le droit à la protection des données exigent souvent l'établissement d'une autorité indépendante chargée de la supervision, afin d'assurer le respect de ces droits et obligations[86]. En raison de la nature procédurale de cette approche, certains ont fait valoir que, contrairement au droit à la protection de la vie privée, le droit à la protection des données n'est pas vraiment un droit substantiel, mais plutôt un droit procédural qui donne finalement effet au droit à la confidentialité des renseignements, en établissant un ensemble de règles détaillées pour son exercice[87]. Pour déterminer si cette situation est véridique, il faut analyser de manière plus détaillée le caractère particulier du droit à la protection des données, ainsi que les éléments qu'il doit protéger.

i. Le lien entre la protection des données et la protection de la vie privée

Certains experts continuent de mettre en doute le fait que la protection des données devrait être un droit fondamental. Par exemple, Veil indique que la protection des données ne devient un droit défensif devant les tribunaux que lorsqu'il est jumelé à un autre droit fondamental. Ainsi, le traitement des données ne serait pertinent en fonction des droits fondamentaux que s'il restreint ou pourrait restreindre de manière précise la liberté[88]. Parmi ceux qui conviennent que la protection des données est un droit fondamental, il existe des conceptions divergentes de sa relation avec le droit à la protection de la vie privée. On peut regrouper ces conceptions en trois (ou quatre) catégories générales[89].

Selon une première conception, les deux droits sont *complètement distincts, tout en étant complémentaires*, dans la mesure où les deux cherchent à réaliser des valeurs plus générales, comme la dignité, l'autonomie ou le contrôle et les limites du pouvoir.

De Hert et Gutwirth indiquent que la protection de la vie privée est un [traduction] « outil d'opacité », qui aide à établir des limites en ce qui concerne les pouvoirs et à empêcher l'exercice illégitime et excessif des pouvoirs, alors que la protection des données est un [traduction] « outil de transparence » qui contrôle les pouvoirs et les canalise au moyen de la transparence et de la reddition de comptes[90].

Une autre conception consiste à considérer *la protection des données comme un sous-ensemble du droit à la protection de la vie privée*. C'est probablement l'opinion la plus courante au sujet de la relation. Par exemple, dans le cas de la Cour européenne des droits de l'homme, on évalue et réglemente la protection des données personnelles en fonction de l'article 8 de la CEDH, c'est-à-dire le droit à la protection de la vie privée. Dans le même ordre d'idées, comme Solove l'indique aux États-Unis, [traduction] « le droit constitutionnel à la confidentialité des renseignements est considéré par les tribunaux comme un dérivé des droits constitutionnels habituels »[91]. Pourtant, même si le droit à la protection des données est un sous-ensemble du droit à la protection de la vie privée, il est possible de faire une distinction entre les situations dans desquelles la protection des données est traitée *comme étant la protection de la vie privée*, et celles où la protection des données a pour but premier de protéger la vie privée[92].

Selon une troisième conception, qui compte un nombre croissant d'adeptes, la *protection des données et la protection de la vie privée sont des droits distincts, mais qui se chevauchent fortement*, alors que la protection des données sert une multitude de fonctions, y compris, mais sans en exclure d'autres, le respect de la vie privée. La protection des données et la protection de la vie privée sont distinctes dans la mesure où elles ont des champs d'application différents; la protection de la vie privée porte sur des domaines que ne cible pas la protection des données, comme les questions d'autonomie corporelle et la vie familiale, alors que la protection des données ne tient pas compte des questions relatives aux « attentes raisonnables » en ce qui concerne la vie privée. Sa protection vise, de manière inconditionnelle, le public et les activités volontaires de traitement de données[93]. L'article 1 de la Convention 108+ tient compte de cette notion, indiquant que le droit à la protection des données est autonome, « contribuant ainsi au respect de ses droits de l'homme et de ses libertés fondamentales et notamment du droit à la vie privée ». Le texte définit le droit à la protection des données comme un droit distinct qui contribue à la mise en application d'autres droits de la personne, tout particulièrement le droit à la vie privée.

Selon une quatrième conception, la protection des données relève d'une obligation positive de l'État. Cette conception est particulièrement pertinente dans certaines instances, comme l'Inde et les États-Unis, où les droits fondamentaux sont structurés principalement sous forme de droits « verticaux », offrant une protection contre les mesures prises par l'État. Inversement, le droit à la protection des données est le plus souvent considéré comme un droit « horizontal » à une protection contre les entités privées[94]. La nature évolutive des droits fondamentaux ne fait pas simplement partie des droits négatifs (c'est-à-dire la protection contre les mesures prises par un État). Il s'agit également de droits positifs, imposant des obligations à l'État quand vient le temps de protéger les droits (contre les entités privées). La protection de la vie privée fait donc l'objet d'une application horizontale indirecte, même dans les instances où les droits fondamentaux ne sont que des

droits verticaux[95]. Selon cette conception, la protection des données n'est pas un sous-ensemble de la protection de la vie privée. Il s'agit plutôt d'une obligation positive de l'État découlant de ses obligations en matière de protection de la vie privée.

Comme de Hert et Gutwirt l'indiquent, [traduction] « on peut trouver peu de manifestations directes des conceptions de la protection de la vie privée axées sur l'intimité dans les dispositions des lois sur la protection des données et, inversement, il n'est pas dans la nature des concepts élargis de protection de la vie privée d'expliquer les principes de la protection des données, comme le principe de finalité, la qualité des données ou la sécurité[96] ». La protection des données accorde aux personnes physiques un éventail élargi de droits en ce qui concerne leurs données par rapport à la protection de la vie privée, y compris des droits à l'accès aux données et même des droits à la portabilité[97]. Pourtant, au fur et à mesure que le champ d'application du droit à la vie privée s'élargit, sur le plan de la jurisprudence, afin de tenir compte des préoccupations à l'ère du numérique, le chevauchement entre ces droits augmente.

Enfin, dans le domaine des droits de la personne au sens large, il y a une reconnaissance mutuelle à savoir que les droits se développent de concert les uns avec les autres et avec la société. Lorsqu'on évalue la hausse de l'importance accordée à la protection des données et à la protection de la vie privée, il est utile de noter qu'un cadre fondé sur les droits reconnaît la nature en constante évolution des droits. Les droits ne sont pas figés dans le temps ni statiques. Ils évoluent au fur et à mesure que la société évolue elle aussi. Cela permet de tenir compte des véritables besoins des personnes physiques en matière de protection, afin qu'elles puissent vivre dans la dignité et le respect. Le droit international en matière de droits de la personne se fonde sur un principe fondamental selon lequel les droits sont interreliés et dépendants. Selon ce principe, si un droit est mieux protégé, les autres pourraient aussi mieux l'être. Dans ce cadre, on pourrait examiner le contexte moderne comme un approfondissement des liens et des dépendances entre la protection de la vie privée, la protection des données et d'autres droits qui apparaissent tout simplement dans la conscience publique et juridique à des rythmes différents et selon un taux de répercussions variable.

ii. Confidentialité des renseignements et autodétermination des renseignements

Sans égard au fait qu'on considère la protection des données comme un sous-ensemble de la protection de la vie privée, comme deux droits « distincts mais qui se chevauchent », ou comme une évolution naturellement interreliée et interdépendante des droits modernes, il existe, sans aucun doute, un chevauchement évident entre les éléments protégés par le droit à la protection des données, comme il est défini dans la Charte de l'UE et certaines constitutions nationales ou d'État, et ce que Westin et Fried ont décrit, à la fin des années 1960, comme la confidentialité des renseignements. Selon Westin, la confidentialité des renseignements est une [traduction] « demande de personnes physiques, de groupes ou d'institutions qui souhaitent déterminer eux-mêmes comment, quand et dans quelle mesure les renseignements à leur sujet sont communiqués à d'autres »[98].

Cette définition de la confidentialité des renseignements comme droit des personnes physiques à déterminer ou contrôler ce qui peut être fait avec leurs données suggère un lien étroit entre ce droit et le droit général à la vie privée. Cela suit le même parcours qu'ont emprunté au XIX^{e} siècle les universitaires américains spécialistes de la vie privée Samuel Warren et Louis Brandeis, qui avaient élargi précédemment le champ d'application du droit à la vie privée, en ajoutant à la dimension physique ou spatiale couramment reconnue une nouvelle dimension réservée à la vie privée qui comprenait la protection des pensées, des sentiments et des émotions d'une personne.

D'autres auteurs, comme Ruth Gavison ou Shoshana Zuboff, font valoir d'autres définitions plus vastes. Ils reconnaissent le déséquilibre actuel des pouvoirs dans les domaines des données et de la vie privée, et reconnaissent que les nouveaux systèmes puissants de collecte et de commercialisation des renseignements numériques sur la vie privée des citoyens sont comparables à d'autres transformations historiques, comme le passage du marché axé sur les terres naturelles au marché de l'immobilier, ou de l'économie de troc aux ressources humaines qui sont une main-d'œuvre régie par le marché[99].

Le droit à l'autodétermination en matière de renseignements (ou la confidentialité des renseignements) et le droit à la protection du domaine privé se fondent sur les mêmes valeurs fondamentales qui soulignent également que, hormis leur origine commune, les deux droits partagent un même objectif, soit la protection de la dignité humaine et de l'autonomie individuelle.

iii. La valeur ajoutée de la protection des données

Lorsqu'on reconnaît qu'il s'agit d'un droit fondamental distinct, on doit se questionner au sujet des valeurs indépendantes que le droit à la protection des données offre aux personnes physiques ou à la société. Comme nous l'avons déjà souligné ci-dessus (et discuté plus amplement ci-dessous), lorsqu'on se pose des questions sur les éléments qu'on protège au moyen du droit à la protection des données, on mentionne souvent l'autodétermination en matière de renseignements.

Au-delà de l'autodétermination en matière de renseignements, certains évaluent la protection des données avec une optique axée sur l'équité et la bonne gouvernance des données[100]. Par exemple, Post suggère que l'article 8 de la Charte de l'UE permet d'appliquer des pratiques justes en matière d'information qui établissent des règles bureaucratiques pour structurer le processus décisionnel des personnes jugées asociales et autonomes[101]. Van der Sloot compare l'idéal athénien de la vie privée aux objectifs de la protection des données qui cherchent à veiller à ce que les données soient utilisées de manière juste et dans le cours normal de la loi[102].

D'autres vont plus loin et donnent à penser que le droit à la protection des données accorde un « droit à une règle » ou un droit à un cadre juridique régissant le traitement des données. En suivant la logique du droit à la protection des données se trouvant dans la Charte de l'UE, ce cadre juridique comprendrait au moins des droits pour les personnes physiques, imposerait des obligations aux personnes chargées du traitement des données personnelles, en plus de mettre en place un mécanisme de surveillance et d'application efficace et indépendant[103]. Ainsi, la

valeur servie par la protection des données revient tout simplement à définir les règles du jeu, afin de faciliter le respect d'autres droits et intérêts[104].

iv. La protection des données comme droit procédural ou droit fondamental

Si un droit indépendant à la protection des données existe pour offrir aux gens un meilleur contrôle sur leurs données personnelles ou garantir l'existence d'un cadre juridique pour le traitement des données personnelles, la protection des données devient-elle ainsi un droit procédural? Certains le pensent, laissant entendre que la protection des données [traduction] « ne constitue pas directement une valeur ou un intérêt en soi; elle prescrit les procédures et méthodes nécessaires pour respecter les valeurs incarnées par d'autres droits[105] ».

Pourtant, il peut être trop réducteur de considérer la protection des données comme un droit purement procédural. En fait, il s'agit d'un droit hybride. S'il cherche à assurer l'autodétermination en matière de renseignements, il s'agit d'une fin en soi, en plus d'être un mécanisme pour garantir la dignité humaine et faire la promotion de la démocratie[106]. Si le droit à la protection des données est un droit à un cadre juridique régissant le traitement des données, on doit reconnaître que certains éléments de ce cadre ont une nature purement procédurale (comme les exigences en matière de transparence et de reddition de comptes), alors que d'autres sont substantiels, exigeant un processus juridique dans le cadre duquel on peut évaluer les intérêts et droits[107]. Même si l'on considère la protection des données comme un droit procédural, n'incarnant aucune valeur indépendante, il n'existe aucune raison justifiant le fait de ne pas la considérer comme un droit fondamental[108].

En fait, l'ONU a reconnu que des droits particuliers, nouveaux ou formulés plus récemment, sont tout aussi fondamentaux. Par exemple, l'article 9 de la *Convention relative aux droits des personnes handicapées* (CDPH) des Nations Unies souligne que le principe d'accessibilité est essentiel pour respecter les droits des personnes en situation de handicap. L'organe créé par traité de la CDPH a souligné que l'accessibilité n'est pas seulement un droit procédural. Il s'agit plutôt de l'expression d'un droit fondamental à l'accès garanti par le PIDCP et le Comité sur les droits économiques, sociaux et culturels (CDESC)[109]. Sa création et sa reconnaissance au fil du temps n'ont pas diminué cette reconnaissance universelle. Dans le même ordre d'idées, la protection des données peut être considérée comme une condition préalable essentielle pour permettre de jouir réellement des droits civils, politiques, économiques, sociaux et culturels de notre ère actuelle, et devrait être reconnue de manière semblable dans le droit international.

Élargissement des droits à la protection de la vie privée : décision dans le cadre du recensement allemand

La Cour constitutionnelle de l'Allemagne a défini un cas pratique pour élargir la signification du droit à l'autodétermination dans le cadre de sa décision source sur le recensement de 1984. La décision a été prise en réaction aux pouvoirs excessifs de collecte et de traitement de données accordés au gouvernement allemand par la *Loi sur le recensement de 1983*. La Cour a créé un nouveau droit à l'autodétermination en matière d'information qui limitait ces pouvoirs. Reflétant, quasiment de manière identique, les sentiments exprimés par Westin au moins 15 ans avant, la Cour a soutenu que la Constitution allemande protégeait précisément le droit de la personne de décider d'elle-même du moment où les détails de sa vie privée peuvent être divulgués et en fonction de quelles limites ils peuvent l'être. En l'absence d'un droit particulier dans la *Loi fondamentale de l'Allemagne*, la Cour a déterminé que ce nouveau [traduction] « droit à l'autodétermination en matière d'information » était un aspect du droit général de la personnalité de la personne physique qui se fondait lui-même sur deux droits existants. Il s'agissait du droit à l'autodétermination prévu au paragraphe 2(1) et du droit à la dignité humaine prévue au paragraphe 1(1) de la *Loi fondamentale de l'Allemagne*. Jusque-là, ce droit de personnalité général, reconnu par la Cour depuis 1973, et avant cela par la Cour civile fédérale depuis 1954, protégeait seulement la personne contre toute immixtion illégale dans le domaine privé. Cependant, au lieu de décrire le droit à l'autodétermination en matière d'information comme un sous-ensemble de ce droit plus ancien, la Cour a accordé aux deux droits un statut égal, mais distinct, avec une origine partagée. Essentiellement, le droit à l'autodétermination en matière de renseignements garantit le droit des personnes à contrôler la divulgation de leurs données personnelles, la manière dont ces données sont utilisées, et à quelles fins elles le sont. La Cour a soutenu que, dans le contexte des procédures modernes de traitement des données, la personne doit être protégée contre les activités illimitées de collecte, de stockage, d'utilisation et de divulgation des renseignements personnels. C'est pourquoi le droit a, de manière traditionnelle, empêché les autorités publiques de se livrer à des activités de collecte et de traitement en vrac de données personnelles ou d'utiliser des identifiants particuliers associés à de telles données pour prendre des décisions qui ont des répercussions juridiques sur les citoyens individuels. Puisque les systèmes de TI modernes peuvent se brancher à d'autres systèmes et regrouper les données, la cour a jugé qu'il n'existe plus de « données non substantielles » (même les données qui semblent elles-mêmes peu pertinentes peuvent devenir pertinentes si elles sont jumelées à d'autres données). Ainsi, la Cour a jugé que la protection des données personnelles ne doit pas dépendre du fait que ces données relèvent du domaine privé ou intime de la personne. Pour évaluer la pertinence du traitement à la lumière d'une contravention potentielle au droit à la dignité et à l'autodétermination d'une personne, il est essentiel de déterminer les fins auxquelles les données sont recueillies et la façon dont elles pourraient être utilisées ou associées à d'autres données. C'est ainsi qu'a surgi l'idée que les données personnelles doivent bénéficier d'une protection accordée aux droits fondamentaux équivalente au droit à la vie privée, même si ces données pourraient ne pas être considérées comme des données « privées ». **Sources :** Loi sur le recensement, BVerfGE 65, 1; traduction anglaise de la Konrad-Adenauer-Stiftung allemande; accessible à l'adresse https://freiheitsfoo.de//files/2013/10/Census-Act.pdf; consulté le 20 octobre 2020.

4. Que protège-t-on lorsqu'on protège la vie privée et la protection des données?

L'élaboration du droit à la vie privée et du droit à l'autodétermination en matière d'information dans le contexte juridique de l'UE (voir ci-dessus) souligne sans doute un aspect qui peut être moins évident dans les mécanismes de droits fondamentaux ultérieurs comprenant un droit exprès à la protection des données. À savoir, la protection de la vie privée, comme concept et comme droit juridique, découle elle-même d'une variété d'intérêts, de droits et de valeurs individuels et publics, et est conçue pour les protéger. Cela comprend le droit de la personne à la réalisation de soi et au développement de sa propre personnalité.

La réalisation de soi comprend le droit de décider comment une personne se présente auprès des autres (p. ex. le contrôle sur son image publique et sa réputation) et la mesure dans laquelle elle se rend accessible et rend sa vie accessible (p. ex. le consentement et le contrôle à l'égard de la publication de détails personnels). Elle porte sur le droit de former et de communiquer des opinions et des convictions sans faire l'objet d'observations indésirables d'autrui (p. ex. le fait de contester les politiques gouvernementales ou de critiquer les décisions politiques). De plus, elle soutient le droit de prendre des décisions et des mesures en fonction de ces opinions et convictions, ce qui peut avoir des répercussions sur la personne, mais aussi sur les intérêts collectifs et publics.

À la base de ces droits, on suppose que sans protection de la vie privée et des données, sans le droit d'interdire à d'autres personnes d'accéder à notre espace, à nos décisions et à nos réflexions, nous ne pouvons pas développer et exprimer notre propre individualité au maximum. En conséquence, on nous empêche de participer à des interactions collectives et à des processus décisionnels en faisant valoir notre soi authentique (p. ex. lorsque des employés se censurent eux-mêmes en milieu de travail par peur de représailles). Cet idéal constitué de l'autodétermination, de la réalisation de soi et du contrôle individuels, exprimés dans le droit général à la protection de la vie privée et le droit à la confidentialité des renseignements, tient donc compte des valeurs plus fondamentales que sont la dignité humaine, la liberté et l'autonomie. Nous allons examiner successivement chacune de ces valeurs.

A. Dignité humaine

La dignité humaine est sans doute la plus importante de ces valeurs, car elle protège l'essence de ce qu'est la vie à titre d'humain, le fait d'avoir une valeur propre et le fait d'être traité avec respect. La Déclaration universelle des droits de l'homme de l'ONU met en évidence l'importance capitale de ce droit, en reconnaissant la dignité inhérente de tous les membres de la famille humaine. C'est aussi le cas de la Convention 108+ et la Charte des droits fondamentaux de l'UE, qui intègrent le respect et la protection de la dignité humaine à son premier article[110]. Le droit à la dignité humaine est également le premier droit énuméré dans la Loi fondamentale de l'Allemagne, en plus d'être l'un des rares droits absolus qui y figurent. Il s'agit de l'un des deux droits inclus dans la Loi fondamentale qu'il est impossible de modifier, sauf si une nouvelle constitution est adoptée. La dignité humaine est donc protégée à titre de valeur éthique et juridique importante. De façon plus pratique, elle renforce

aussi les interdictions visant les pratiques inhumaines que sont l'esclavage, la torture et la traite de personnes.

L'exigence selon laquelle il faut traiter chacun comme une personne en respectant son humanité et ne pas lui faire subir de traitement inhumain tient compte du concept moral de Kant en matière de dignité, à savoir qu'il faut agir « de telle sorte que tu traites l'humanité aussi bien dans ta personne que dans celle de tout autre toujours en même temps comme une fin, et jamais simplement comme un moyen »[111]. Cette exigence a des répercussions immédiates, c'est-à-dire que personne ne devrait être utilisé comme moyen pour parvenir à d'autres fins.

Cependant, certains ont mentionné que cette possibilité peut être préoccupante en ce qui concerne les pratiques de traitement des données personnelles qui peuvent faire des personnes de simples objets. Par exemple, Lyon signale que l'utilisation de plus en plus intensive des données personnelles par les ordinateurs pourrait simplement faire des personnes des marchandises et soumettre les valeurs humaines à la seule efficacité[112]. Citron et Pasquale ont des préoccupations semblables, montrant que les pratiques actuelles de l'évaluation fondée sur les données pourraient faire des personnes physiques des objets notés et classés[113]. De nombreux universitaires œuvrant dans le domaine des études sur la surveillance ont critiqué vertement la protection de la vie privée, à titre de discours et de régime de gouvernance[114]. Selon eux, elle ne réussit pas à rétablir l'équilibre des pouvoirs. Ils se méfient des protections juridiques et constitutionnelles d'un droit à la vie privée.

Dignité humaine, tri social et numérisation

Parmi les phénomènes illustratifs dans ce contexte, il y a la cote de solvabilité. Dans les secteurs financiers, il est possible que des économies puissent être réalisées en raison de l'utilisation de mégadonnées (y compris l'utilisation de renseignements autres que sur le crédit, comme les réseaux sociaux ou les tendances en matière d'achat ou de navigation) pour évaluer la cote de solvabilité, car les données peuvent servir à déterminer les tendances relatives à un défaut de paiement potentiel qui s'appliquerait correctement à la plupart des clients. Cependant, toute personne qui correspond apparemment aux critères des tendances, mais qui, en fait, est peu susceptible de ne pas faire de paiements sera pénalisée par cette catégorisation, car elle n'est pas traitée comme elle aurait dû l'être en fonction de sa propre situation. On fait plutôt abstraction de sa situation personnelle dans l'intérêt des stratégies de maximisation des revenus de l'entreprise. De même, des entreprises et d'autres utilisateurs de données peuvent ne pas tenir compte du fait que les données brutes utilisées par leurs algorithmes de prise de décisions peuvent être inexactes ou dépassées. Cette situation pourrait ne pas seulement toucher la personne en question. Elle pourrait aussi avoir une incidence sur le développement plus avancé de l'algorithme lui-même, surtout lorsque les données brutes font partie d'un ensemble de données servant à la formation. Cela pourrait avoir des conséquences à long terme sur les personnes sur lesquelles l'algorithme a des effets pratiques ou juridiques. Enfin, à l'ère de l'apprentissage automatique, les algorithmes sont conçus pour « améliorer » le programme initial en fonction des données fournies. Les entreprises peuvent ne plus être en mesure de déterminer les critères que l'algorithme utilise, donnant lieu à des scénarios du type « l'ordinateur dit non », où le processus décisionnel algorithmique échappe à la reddition de comptes et les biais algorithmiques potentiels visant des types particuliers de personnes deviennent indécelables en pratique, résistant à la surveillance réglementaire. On examine de manière plus détaillée l'opacité du processus décisionnel algorithmique à la page 41. [Please check p. number in English and French versions]

La cote de solvabilité n'est qu'un exemple parmi d'autres[115]. Tous ces cas montrent que la *mise en données* des personnes d'une manière ne permettant pas à ces personnes de contrôler ces données fait état d'un non-respect des personnes à titre d'humains qui va à l'encontre de la dignité humaine, car les utilisateurs de données ne se soucient aucunement du bien-être de ces personnes ni de leur droit à un traitement équitable. Au cours des deux dernières décennies, les transformations en ce qui concerne l'envergure de la collecte de données numériques, ainsi que l'étendue de leur portée mondiale et de leurs capacités de stockage, mettent en évidence un déséquilibre flagrant en ce qui concerne le contrôle de l'information. Les déséquilibres de pouvoir en découlant (attribuables à la numérisation et aux marchés de données) représentent un risque pour les droits politiques, sociaux, économiques et culturels (pas seulement la dignité humaine)[116]. Les déséquilibres du pouvoir en jeu et la portée des préjudices potentiels constituent un argument solide quand vient le temps d'expliquer pourquoi la protection de la vie privée devrait être un droit de la personne clairement défini. Le droit à la protection des renseignements qui augmente le contrôle qu'une personne exerce sur ses données est ainsi considéré comme une façon de se protéger contre de telles violations.

B. Liberté et autodétermination

L'objectif visant à protéger les personnes physiques de l'immixtion des organismes gouvernementaux, en tenant particulièrement compte de l'existence actuelle d'une surveillance électronique répandue, a orienté la majorité de la discussion sur le droit à la vie privée. Dans ce contexte, le droit à la protection des renseignements cherche à protéger la valeur sans doute encore plus fondamentale qu'est la « liberté » comme droit ultime de la personne de ne pas être soumise à une telle immixtion de l'État. En effet, Lyon a fait valoir qu'il est préférable d'utiliser le terme liberté, au lieu de vie privée, lorsqu'on parle des tendances totalitaires au sein d'une société fondée sur la surveillance[117]. Même si la signification exacte de liberté n'est pas immuable, on considère généralement qu'il s'agit du droit naturel intégral des gens de suivre leur propre désir[118]. Dans ce contexte, les métaphores que sont les expressions « Big Brother » et « bâtiment

panoptique » sont habituellement considérées comme une limite imposée au libre arbitre de chacun au moyen de la surveillance évidente et réelle. Il est aussi possible que des personnes physiques croient qu'ils sont observés sans pouvoir indiquer avec exactitude quand et dans quelles conditions la surveillance est réalisée[119]. Dans les deux cas, selon cet argument, les personnes adapteront leur comportement en fonction des règles et attentes de l'observateur.

C. Autonomie et choix

Enfin, la notion de protection de la vie privée comme contrôle individuel est sans doute étayée par les concepts d'autonomie et de choix. Selon la théorie libérale, les personnes physiques sont d'abord et avant tout des agents autonomes qui assurent la réalisation de soi au moyen de décisions même banales[120]. L'idée de la dignité humaine et celle de la liberté individuelle suggèrent que nous devrions être les auteurs de notre propre histoire, « maîtres de notre destinée » et « capitaines de notre âme »[121]. Selon les cadres économiques libéraux, les choix des consommateurs sur le marché sont des choix libres, car ils supposent que les deux parties ont des renseignements exhaustifs, que le choix cohérent suppose le fait d'avoir des renseignements complets et un degré de transparence.

Cependant, en réalité, nos décisions se fondent sur un délicat équilibre entre les contraintes et les choix. Elles sont déterminées par les environnements économiques, sociaux et politiques particuliers dans lesquels nous évoluons. Dans l'environnement actuel, l'État et le secteur privé qui recueillent des mégadonnées sur les citoyens, les échangent et les utilisent, disposent d'un énorme avantage en matière d'information, en plus de bénéficier d'un degré d'opacité en ce qui concerne la manière dont ils utilisent ces données[122]. De plus, un examen actuel des formulaires de consentement en ligne met en évidence le fait que les citoyens et les consommateurs peuvent ne pas avoir de véritable choix ni avoir l'autonomie nécessaire pour refuser que leurs renseignements soient recueillis et utilisés à l'avantage des entreprises et États et au désavantage des consommateurs et des citoyens[123]. Même au sein de démocraties, ces données peuvent être exploitées pour manipuler de manière opaque les électeurs, à leur insu ou sans leur consentement. On peut considérer les droits et l'application de règles équitables pour assurer leur respect comme une façon d'offrir un degré supérieur d'autonomie et des choix plus significatifs.

En tant que personnes, nous n'existons pas en vase clos. Nous ne prenons pas de décisions hors des structures de pouvoir en place qui nous confèrent des privilèges ou nous désavantagent (ou parfois les deux de différentes manières). En vérité, l'autonomie est liée par l'intérêt personnel existentiel, les dépendances économiques, nos relations avec les autres, nos obligations envers ces derniers et le pouvoir relatif (ainsi que toute responsabilité, comme nous l'avons mentionné ci-dessus) que nous pouvons avoir à titre de membres de nos communautés respectives. On présente chacun de ces éléments aux fins d'évaluation et de réflexion dans une annexe au présent exposé.

5. La protection de la vie privée et la protection des données comme droits individuels ou collectifs

L'élément « communautaire » des droits à la vie privée et à la protection des données prête un peu à controverse. D'une part, le statut de ces droits comme droits individuels dans les instruments sur les droits de la personne les plus libéraux a été vivement critiqué par les partisans du communautarisme et les défenseurs de l'adoption d'une approche davantage axée sur les intérêts collectifs ou sociétaux. Cependant, cette critique comporte sa part de défis. Si la protection de la vie privée constitue essentiellement un [traduction] « droit à ne pas participer à la collectivité » et à [traduction] « isoler la personne de divers types d'ingérences »[124], alors comment peut-elle être utilisée de manière fiable pour promouvoir les besoins de la communauté? D'autre part, comment la vie privée en tant que « droit d'être laissé tranquille » (Warren et Brandeis) interagit-elle avec la [traduction] « valeur sociale » de la vie privée (Priscilla Regan)[125]?

Une approche combinant la marchandisation des données à une conception de la vie privée et de la protection des données comme un outil visant uniquement à faciliter le contrôle individuel peut convaincre plus facilement les personnes, les entreprises et les législateurs de la valeur intrinsèque et de la légitimité de certains [traduction] « compromis en matière de vie privée »[126]. Comme nous l'avons déjà expliqué, le [traduction] « risque d'atteinte à la vie privée » lié à une activité de traitement, qu'elle soit effectuée par des contrôleurs du secteur public ou privé, ne sera perçu que comme un risque parmi d'autres, comme les menaces existentielles, le préjudice économique et la crainte de l'exclusion sociale.

Dans la pratique, les personnes peuvent justifier plus facilement le traitement des données (à eux-mêmes et aux autres) qu'elles considèrent comme servant les intérêts supérieurs des personnes physiques, des entreprises et des communautés. Par ailleurs, cela signifie aussi que la protection de la vie privée et la protection des données comme droits fondamentaux sont souvent considérées comme secondaires par rapport à d'autres droits et libertés. Le droit à la vie, à la liberté d'expression et à la liberté de la presse ne sont que trois exemples courants. De même, l'intérêt public qui concurrence la protection de la vie privée ou l'emporte sur celle-ci comprend l'ordre public, la sécurité nationale ou la santé publique, qui bénéficient manifestement à la fois aux intérêts individuels, collectifs ou sociaux.

A. Différences culturelles?

Parallèlement, on laisse souvent entendre que l'idée de « protection de la vie privée » comme droit individuel est une interprétation libérale qui ne correspond pas bien aux traditions culturelles, historiques, religieuses et philosophiques qui façonnent les visions du monde des communautés, surtout dans certaines parties de l'Afrique, dans certaines parties des économies de l'Asie-Pacifique, et dans les régions où l'histoire coloniale a porté préjudice aux populations autochtones, comme au Canada et en Australie.

Des régions et des régimes très différents débattent de questions de droits, de responsabilités et de réparations selon leur propre histoire et expérience sociétale.

Reconnaître ces divergences et ces nuances est une condition préalable et non un obstacle pour comprendre comment améliorer la protection des données. La mise en place de tout écosystème réglementaire, que ce soit dans l'UE, en Amérique du Nord ou en Amérique latine, représente une évolution consciente et une négociation délibérée. Aucun n'a vu le jour « naturellement » et aucun n'est « inévitable ».

En fait, de nombreux pays (en Asie-Pacifique, en Afrique et en Amérique latine) qui envisagent l'adoption ou la révision de leur régime de protection des données le font sans être *gênés* par l'histoire et la philosophie qui ont sous-tendu l'adoption de la première génération de lois sur la protection de la vie privée[127]. Comme nous l'avons mentionné (voir « Origines du droit à la vie privée »), la plupart étaient des réactions législatives propres à des pratiques de surveillance gouvernementale liées à la Seconde Guerre mondiale et au début de la Guerre froide.

En revanche, les sociétés dans les pays en développement ont été très éloignées de ces conséquences. Leurs gouvernements ont plutôt travaillé à la reconstruction et au développement d'une économie mondialisée et à l'intégration dans celle-ci afin d'offrir un meilleur avenir à leur population[128]. À cet égard, les gouvernements et leurs citoyens appuient activement l'innovation, la numérisation et le partage transfrontalier des données[129]. Ces points de vue et priorités doivent être reconnus, validés et appuyés plutôt que marginalisés, négligés ou exclus[130].

Pour ne citer qu'un exemple de cette complexité, la région de l'APEC compte plusieurs traditions, systèmes juridiques, et modèles politiques et socioéconomiques. Cette diversité dépasse même celle de l'Europe ou des Amériques, et des débats sur la vie privée sont en cours. Par exemple, les discussions du sommet d'Osaka en juin 2019 ont ravivé les tensions sous-jacentes sur la gouvernance des données, alors que de nombreux pays asiatiques empruntent des voies différentes sur les problèmes cruciaux liés aux données[131]. L'Inde a notamment fait valoir que toute réglementation sur la gouvernance des données en dehors de l'Organisation mondiale du commerce (OMC) réduirait le pouvoir des économies émergentes dans le débat et supprimerait leur droit souverain d'établir des règles favorisant l'intérêt supérieur de leurs citoyens[132].

Dans la pratique, les lois sur la protection des données ont été élaborées de façon inductive en Asie comme dans les autres pays qui vivent sous l'influence du taoïsme, du bouddhisme et du confucianisme (p. ex., la Corée ou le Japon) et qui ont adopté de telles mesures depuis des décennies[133]. Par exemple, la loi coréenne sur la protection des renseignements personnels a la réputation d'être l'une des plus sévères au monde en matière de protection des données. Ces divergences ne sont donc pas simplement économiques et politiques; elles peuvent s'étendre aux conceptions philosophiques et sacrées des sociétés.

Kitiyadisai explique qu'il est notamment difficile d'harmoniser le concept libéral occidental de vie privée comme un droit individuel aux valeurs bouddhistes, car le bouddhisme perçoit les concepts de droits de la personne et de la protection de la vie privée comme des règles créées par l'homme qui entreraient [traduction] « inévitablement en conflit en elles-mêmes, car elles sont créées pour servir l'avarice humaine ». Comme ces règles [traduction] « reflètent la force dominante dans la société », elles [traduction] « entraîneraient une concurrence accrue et des attitudes

agressives pour protéger et promouvoir les intérêts de divers groupes »[134]. Autrement dit, des éléments de certaines cultures et sociétés peuvent percevoir les droits de la personne, dont la protection de la vie privée et la protection des données, comme des outils qui reflètent et appuient les structures de pouvoir existantes plutôt que de les remettre en question.

Dans le contexte africain, Olinger et Britz ont affirmé que [traduction] « la notion de vie privée ne fonctionne pas dans la pensée philosophique africaine », car elle est en contradiction avec le concept d'*ubuntu*[135]. *Ubuntu*, que l'on traduit souvent par « Je suis, car tu es », est souvent décrit comme une forme particulière d'humanisme africain qui priorise le communautarisme et l'interdépendance à l'individualisme et la concurrence. Ainsi, [traduction] « la vie privée brille par son absence en tant que valeur ou droit cher aux sociétés ubuntu », car [traduction] « un droit individuel ne sera accepté que s'il sert la communauté »[136].

Bien que cette critique du droit à la vie privée semble chevaucher les variantes de certaines des autres régions énumérées ci-dessus, elle fait ressortir un problème auquel les défenseurs de la protection de la vie privée et de la protection des données sont aussi confrontés partout : il a toujours été [traduction] « difficile de faire valoir l'avantage social de la vie privée »[137]. Cependant, étant donné les éventuels inconvénients d'une absence croissante de vie privée, causée par une appropriation généralisée des données par les nouvelles technologies et les nouveaux modèles commerciaux, non seulement sur une personne, mais sur les intérêts collectifs et sociaux, nous estimons qu'il est temps de plaider en ce sens[138].

De plus, les questions relatives aux diverses conceptions culturelles de la vie privée sont liées au domaine philosophique. Tout au long de l'histoire, il a été possible d'observer la problématique de notre humanité courante par rapport à la différence culturelle. De même, il est possible de remonter jusqu'à l'ancien problème philosophique de l'un et du multiple, que l'on retrouve dans de nombreux domaines d'application[139]. Pour comprendre la différence (le multiple), nous devons avoir une idée du commun ou de l'identité. Tout comme la signification de l'idée du commun (l'un) dépend de la différenciation (le multiple). Cette analogie vaut autant pour les concepts de vie privée, car le privé n'est compréhensible que dans le concept de public, qui lui n'a de sens que par rapport à ce qui est privé[140]. À vrai dire, il est donc impossible d'avoir une vie publique et collective significative sans avoir une vie privée individuelle[141].

Ces différences de vision du monde existent aussi dans les démocraties modernes, surtout là où vivent les peuples autochtones, et elles ont inspiré l'élaboration d'un instrument international, la *Déclaration des Nations Unies sur les droits des peuples autochtones*. Les droits et la vision du monde de divers peuples autochtones sont passés au-devant de la scène dans de nombreuses régions du monde, tout comme l'importance de respecter ces droits, d'adapter les lois et d'amorcer la réconciliation dans les nations touchées de manière horrible et injuste par le colonialisme. Cette vision du monde englobe de nouvelles interprétations des droits individuels et collectifs. Tout nouvel instrument international ou règlement national devrait donc prendre en compte et consulter les Autochtones qui y vivent.

B. Préjudices individuels, collectifs et sociétaux

Il a longtemps été difficile de présenter des arguments convaincants en faveur d'une interprétation des droits à la vie privée et à la protection des données qui inclut un point de vue communautaire ou social. Cette difficulté s'explique en grande partie par le fort accent mis par la pensée libérale occidentale sur les droits fondamentaux en tant que droits individuels, où une ingérence doit toujours entraîner un préjudice vérifiable pour la personne[142]. Le concept de « préjudice » dans le droit à la vie privée et à la protection des données est complexe et contesté. Certains avancent que pour ouvrir droit à une poursuite, il doit y avoir un certain préjudice matériel ou une certaine atteinte à la réputation, alors que d'autres indiquent que le concept de préjudice doit être directement lié à un risque précis et au temps qu'il lui faut pour se matérialiser.

Par exemple, dans le contexte des discussions sur la conservation obligatoire des données de communication aux fins d'application de la loi, les autorités ont souvent soutenu que la simple collecte et conservation de données ne pose aucun risque et qu'il n'y a donc aucune atteinte au droit à la vie privée et à la protection des données tant que ces données ne sont pas consultées. En Europe, cet argument a été rejeté par la CJUE dans *Digital Rights Ireland* et la jurisprudence subséquente[143], mais il l'emporte dans de nombreux autres contextes[144].

Le problème de cette approche est qu'elle s'articule uniquement autour d'un concept d'atteinte à la vie privée qui est à la fois économique et individualisé. Selon cette approche, il n'y aura préjudice que si la personne concernée subit un dommage ou une détresse (économiques) vérifiables. Or, les développements des dernières années ont montré que cette conceptualisation de l'atteinte à la vie privée est insuffisante. La seule raison n'est pas son parti pris économique, mais aussi son défaut de tenir compte de nombreux risques et préjudices subis non pas par la personne concernée, mais par d'autres personnes (souvent celles avec lesquelles la personne concernée partage certaines caractéristiques) et par l'ensemble de la société.

En revanche, une approche axée sur les droits de la personne tient compte des préjudices non économiques, comme l'atteinte à la dignité humaine. Les droits de la personne sont aussi un droit public et reconnaissent qu'une atteinte aux droits d'une personne est aussi un préjudice au bien public. Quand on envisage la protection de la vie privée et la protection des données comme des droits fondamentaux, on doit donc aussi tenir compte des préjudices moins « visibles » et de la mesure dans laquelle ils portent atteinte aux intérêts individuels, collectifs et sociétaux.

Comme l'autonomie décisionnelle est un principe clé du droit à la vie privée, les intérêts collectifs reposent sur l'idée d'autodétermination, désormais reconnue comme un principe fondamental du droit public international. Bien que d'abord formulés comme un principe politique à l'époque de la décolonisation, les aspects internes de l'autodétermination ont récemment acquis une plus grande importance. Shaw a décrit l'autodétermination comme « la poursuite par un peuple de son développement politique, économique, social et culturel dans le cadre d'un État existant »[145].

i. Préjudices invisibles

La capacité des entités publiques et privées à recueillir de grandes quantités de données dans divers contextes, à les combiner à d'autres données, et à les analyser rapidement a mené à la libre circulation des données personnelles. Nos renseignements traversent des portes tournantes : d'organismes publics à organismes privés (et vice versa), entre organismes publics et entre organismes privés, sans que l'on ne se soucie guère des fins auxquelles ils ont été recueillis au départ. D'ailleurs, de plus en plus de pressions s'exercent sur les autorités publiques afin qu'elles partagent avec le secteur privé les données administratives qu'elles détiennent pour promouvoir « l'innovation ». L'attitude qui prévaut dans de nombreuses pratiques de traitement contemporaines semble être : [traduction] « si les données sont déjà là, nous devrions pouvoir les utiliser »[146].

Non seulement cette approche illustre clairement l'existence de la « base de données de ruines » d'Ohm, à savoir le risque que des données auparavant anonymes soient sujettes à une réidentification par leur combinaison avec d'autres données, mais elle souligne aussi les atteintes invisibles à la vie privée qui peuvent se manifester en cas de violation de l'intégrité contextuelle de la divulgation de renseignements personnels[147]. Comme on l'a dit précédemment :

> [traduction]
>
> *Du point de vue des personnes concernées, il est désormais quasi inévitable que, tôt ou tard, les données qu'elles divulguent à une entité soient partagées entre deux ou plusieurs entités publiques ou privées sans leur consentement explicite et souvent à leur insu. Il devient donc impossible pour la personne concernée de savoir lors de la collecte combien de temps ses données seront conservées, comment elles seront utilisées dans le futur, à quelles fins et par qui. Lors de la divulgation de leurs données, les personnes concernées ne peuvent donc pas prendre une décision éclairée quant aux risques liés à cette divulgation ni de précautions raisonnables contre ces risques*[148]*.*

Voilà qui représente une modification de l'équilibre du « pouvoir de l'information » en faveur de l'entité déjà plus puissante (habituellement l'entreprise ou l'organisme public) qui facilite la marchandisation des personnes, permet la discrimination et [traduction] « par-dessus tout [...] subordonne les considérations de bien-être et d'autodétermination de la personne aux priorités et aux valeurs de puissants protagonistes »[149]. Ainsi, nous avons pu observer une perte de contrôle des personnes sur l'autoarticulation[150].

De même, les pratiques actuelles de traitement des données font de plus en plus abstraction du principe de minimisation des données qui a longtemps été la pierre angulaire du cadre de protection des données de l'UE et du Conseil de l'Europe)[151]. Ce cadre prévoit que les données personnelles doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont recueillies ». Pourtant, trop souvent, l'attitude des contrôleurs de données dans les secteurs public et privé est plutôt : « toutes les données, tout le temps ».

Dans le contexte commercial, Shoshana Zuboff a décrit ce processus comme le [traduction] « capitalisme de surveillance », qui [traduction] « revendique unilatéralement l'expérience humaine comme matière première gratuite » qui sera ensuite [traduction] « traduite en données comportementales » et [traduction] « transformée en produits de prédiction[152] ». Cette adaptation de l'expérience utilisateur à ses préférences connues permet sans doute un niveau de manipulation sans précédent. Dans le cas le plus bénin, il peut y avoir une hausse des ventes d'une entreprise à un client ou une simplification de la prestation de services publics[153]. En revanche, elle peut aussi coincer les personnes dans un environnement où leurs préjugés sont à la fois renforcés et amplifiés, où ils ne sont plus exposés à différents biens, services, renseignements, points de vue ou expériences, ou encore où ils sont poussés vers des points de vue privilégiés par l'État ou d'autres organisations dans le but de porter atteinte à des droits fondamentaux comme le droit de vote ou de se forger une opinion[154].

ii. Préjudices collectifs et sociétaux

En plus des conséquences directes que les nouvelles pratiques en matière d'utilisation des données peuvent avoir sur les personnes, nous devons aussi tenir compte de leur possible effet à long terme sur les intérêts collectifs et sociétaux. Des préjudices collectifs peuvent surgir quand le traitement des données personnelles d'une personne a une incidence sur d'autres personnes avec lesquelles elle partage certaines caractéristiques ou particularités. C'est généralement le cas quand une analyse de modèle est effectuée sur les données personnelles recueillies auprès d'un nombre suffisant et représentatif de personnes, ce qui permet de tirer des conclusions qui s'appliqueront aussi aux autres membres du même groupe, même si leurs données n'étaient pas disponibles pour une analyse directe. Par exemple, sur le plan psychologique ou émotionnel, les tests psychométriques peuvent trouver les partis pris et les vulnérabilités de certains types de personnes, ce qui peut s'avérer utile pour « pousser » ces personnes et d'autres qui partagent les mêmes caractéristiques à adopter certains comportements souhaitables ou avantageux.

Sur le plan physiologique, les résultats de tests d'ADN, souvent obtenus par des personnes pour leur référence personnelle, peuvent être utilisés dans un contexte de recherche pour déterminer si une personne est susceptible de contracter une certaine maladie. Entre les mains de spécialistes en commercialisation, de professionnels de la santé et de compagnies d'assurance, de tels renseignements pourraient orienter les décisions quant au type de produits et de médicaments, aux primes d'assurance ou aux accès à certains services de santé à proposer aux personnes avec des caractéristiques similaires. De même, les données personnelles divulguées particulièrement pour obtenir un avantage financier ou matériel peuvent ensuite être utilisées pour susciter des attentes chez l'utilisateur des données (comportements souhaitables ou acceptables) qui sont ensuite imposées à d'autres personnes qui n'ont pas consenti à ce type de compromis financier ou matériel. Dans le cycle de vie des données, ce type de divulgation commence souvent comme un moyen d'obtenir un certain incitatif, mais évolue rapidement pour devenir la norme généralement adoptée et incontestée jusqu'à ce qu'elle se transforme en un outil d'exclusion.

Il peut y avoir des préjudices sociétaux quand le traitement des données personnelles d'une personne contribue à des collectes de données ou facilite des activités de traitement des données qui rendent difficile, voire impossible, l'exercice des droits et devoirs démocratiques, ou quand elles permettent de manipuler des personnes et des groupes d'une manière susceptible de modifier les rapports de force dans la société. L'effet paralysant de la surveillance omniprésente des

communications est souvent cité en exemple pour la première possibilité. Les personnes qui savent que leurs communications sont interceptées ou peuvent l'être n'utiliseront pas certains moyens de communication pour des utilisations particulières. Par exemple, en République démocratique allemande (Allemagne de l'Est), il était entendu qu'il fallait « éviter le téléphone » pour certaines conversations. Pourtant, ce changement de comportement peut aussi avoir des incidences plus vastes sur la participation politique, la résistance et la résilience générale d'un corps politique.

En parallèle, les outils de surveillance capitaliste décrits ci-dessus (suivi en ligne, profilage, ciblage, hiérarchisation) peuvent être utilisés pour cibler certains messages selon les préjugés de chaque personne et ainsi les encourager à adopter certains comportements ou à ne rien faire du tout. Bien qu'il soit encore contesté que le ciblage politique ait en fait réussi à influencer le comportement des gens (par exemple, sur leur vote lors de l'élection présidentielle américaine ou du référendum britannique sur le Brexit de 2016), il est clairement en mesure d'amplifier certains types d'information et d'en supprimer d'autres[155].

Les véritables préjudices sociétaux découlent tout simplement de notre incapacité à déterminer pleinement le risque réel posé par ces techniques et donc à nous en défendre. Dans des contextes comparables où le préjudice causé par un dispositif, un processus ou un comportement, s'il se manifestait, était désastreux pour la société ou ses valeurs, le résultat fut traditionnellement des appels à l'utilisation du « principe de précaution »[156]. Par contre, dans le contexte de l'information, nous sommes souvent confrontés à une situation où [traduction] « les entreprises du secteur de l'information [...] ont commencé à développer un nouveau cadre métaphorique qui positionne l'environnement d'information et de communication en réseau comme un appareil dépolitisé et autorégulé pour la production de la vérité », alors qu'en réalité, il n'est ni l'un ni l'autre et qu'il a plutôt [traduction] « provoqué des virages profonds dans les relations de responsabilité »[157]. L'élaboration d'un discours alternatif et efficace dépend donc de l'accent mis non seulement sur la valeur *individuelle*, mais aussi *publique et collective de la protection de la vie privée et des données*.

C. La valeur publique et collective de la protection de la vie privée et des données

Les pionniers de la réflexion sur la protection de la vie privée ont toujours reconnu que l'action (ou l'inaction) des personnes qui contrôlent (ou non) l'accès à leurs données risque d'avoir une incidence non seulement sur leurs propres intérêts, mais aussi sur les droits d'autrui et l'intérêt public. Parmi les premiers chercheurs américains à s'être penchés sur cette question, Regan a indiqué dès 1995 que, dans

une société de plus en plus dépendante de la technologie, [traduction] « la vie privée devient moins un attribut des personnes et des dossiers et plus un attribut des relations sociales et des systèmes d'information ou de communication »[158].

Elle affirme qu'en plus d'être une valeur individuelle, la protection de la vie privée est aussi une valeur publique et collective, et explique que la valeur collective de la protection de la vie privée joue un rôle clé dans le soutien des institutions et des pratiques démocratiques. Ces distinctions entre la protection de la vie privée en tant que valeur collective, publique et commune, prennent un sens très différent dans son cadre. Anticipant les plus récents développements relatifs aux préjudices collectifs et sociétaux causés par les activités de traitement des données fondées sur le consentement individuel, elle affirmait déjà à l'époque qu'il existe un risque que [traduction] « si une personne ou un groupe renonce à son droit à la vie privée, le niveau de protection de tous diminue, car la valeur de la vie privée diminue »[159].

Plus tôt encore, en 1987, Spiros Simitis avançait que [traduction] « les formes modernes de traitement des données ont modifié le débat sur la vie privée de trois manières principales »[160]. Premièrement, elles expriment des conflits qui touchent tout le monde, mais d'une manière qui les représente comme des préoccupations individuelles. Deuxièmement, grâce aux nouvelles technologies, elles permettent d'enregistrer et de reconstituer les activités individuelles dans les moindres détails, ce qui systématise la surveillance perpétuelle. Troisièmement, elles sont de plus en plus utilisées pour faire appliquer des normes de comportement, conférant ainsi un pouvoir supplémentaire à ceux qui sont en mesure de déterminer quelles devraient être ces normes. Ces trois développements se sont concrétisés dans l'omniprésence du suivi du comportement en ligne des personnes, la création de profils détaillés à leur sujet et l'utilisation de ces profils pour influencer leurs croyances et leurs décisions commerciales et politiques[161].

Se référant à la décision de la Cour constitutionnelle allemande concernant le recensement de 1984, Simitis souligne à quel point la protection de la vie privée facilite l'exercice d'autres droits, dont la liberté d'expression, d'association et de réunion. Étant donné qu'aucun de ces droits [traduction] « ne peut être pleinement exercé tant que l'on ne sait pas dans quelles circonstances et à quelles fins les renseignements personnels sont recueillis et traités », il affirme qu'une perte de vie privée sera toujours une perte de [traduction] « qualité démocratique »[162]. La protection de la vie privée doit devenir plus que la protection de n'importe quel droit. Au contraire, le niveau de protection accordé aux personnes peut [traduction] « déterminer le choix entre une société démocratique et autoritaire »[163].

La Cour a fait valoir le même point dans sa décision[164]. Elle a notamment fait remarquer que les personnes qui ne sont pas certaines si leur comportement est observé par ceux qui les gouvernent pourraient être grandement freinées dans l'exercice d'autres droits généralement perçus comme des droits importants de la participation politique (y compris, par exemple, leur liberté d'association ou de réunion)[165]. Selon la Cour, ce ne sont pas uniquement les personnes qui sont touchées. Au contraire, l'autodétermination informationnelle est [traduction] « un préalable essentiel au fonctionnement d'une société démocratique libre fondée sur la liberté d'action et de participation de ses membres ». Contrairement aux concepts traditionnels de liberté et d'autodétermination, la Cour a considéré que ces droits

n’existaient pas pris individuellement. La liberté individuelle et l’intérêt public (dans l’existence d’une société libre) sont plutôt présentés comme des objectifs égaux de la protection constitutionnelle.

6. Relation entre la protection de la vie privée et d'autres droits et valeurs

Les droits à la vie privée et à la protection des données ne sont pas absolus. Un des principes fondamentaux des droits de la personne est qu'ils sont tous interreliés et interdépendants. Des ingérences dans ces droits et des dérogations à ces droits sont possibles pour concilier la protection de la vie privée et des données avec d'autres droits et intérêts de la société. Dans son observation générale sur l'article 17 du PIRDCP, le CDHNU indique qu'il ne faut pas compromettre la vie privée, à moins que ce soit motivé par la loi et indispensable dans l'intérêt de la société[166].

De même, l'article 8 de la CEDH reconnaît que toute ingérence dans le droit au respect de la vie privée est permise pourvu qu'elle poursuive un but légitime, qu'elle soit conforme à la loi et qu'elle soit proportionnelle, soit qu'elle n'aille pas au-delà de ce qui est nécessaire pour atteindre ce but. Ces clauses restrictives garantissent que les droits à la protection des données et à la protection de la vie privée font place à d'autres droits et intérêts lorsque c'est souhaitable, mais uniquement dans la mesure nécessaire à leur exercice[167].

Pour citer un exemple de ces interactions, prenons l'article 27 de la DUDH qui dispose que « toute personne a le droit […] de participer au progrès scientifique et aux bienfaits qui en résultent ». Avec les protocoles de recherche actuels, il n'est pas difficile d'imaginer des scénarios où une personne serait contrainte de renoncer à des données personnelles afin de partager l'innovation scientifique de l'ère numérique; ce serait peut-être une violation de l'article 27. De même, l'article 29 stipule que « dans l'exercice de ses droits et dans la jouissance de ses libertés, chacun n'est soumis qu'aux limitations établies par la loi exclusivement en vue d'assurer la reconnaissance et le respect des droits et libertés d'autrui et afin de satisfaire aux justes exigences de la morale, de l'ordre public et du bien-être général dans une société démocratique ».

Tout cela pour dire que même la vie privée comme droit fondamental doit être replacée dans son contexte. Comme nous l'avons indiqué précédemment, non seulement la protection de la vie privée et la protection des données personnelles peuvent être conciliées avec d'autres droits et intérêts, mais dans diverses circonstances, le respect de ces droits est essentiel ou, du moins, facilitera la réalisation d'autres droits et intérêts pertinents, comme la liberté d'expression. Un autre exemple est le droit de se former et d'avoir librement une opinion en vertu de la DUDH (article 19), où un lien clair est établi entre la protection de la vie privée et les droits à l'autonomie et à la formation d'opinion[168]. Ces droits pourraient donc être classés à juste titre comme des droits relatifs et habilitants.

A. Sécurité

La sécurité publique et nationale est le plus souvent citée comme un droit qui entre en conflit avec les droits à la vie privée et à la protection des données. C'est particulièrement vrai depuis les attentats du 11 septembre 2001 aux États-Unis, qui ont mené à l'adoption d'une panoplie de nouvelles lois accordant aux services d'application de la loi, de sécurité et du renseignement de vastes pouvoirs pour

recueillir et traiter les données personnelles des citoyens. En effet, la sécurité nationale est un des intérêts explicitement énumérés dans de nombreux instruments de défense des droits de la personne comme motif de restriction de droits, comme la protection de la vie privée et la protection des données[169].

Les instruments et les tribunaux de défense des droits de la personne ont mis en place de solides mesures de protection substantielles et procédurales afin de limiter l'ingérence des services d'application de la loi et de sécurité à ce qui est nécessaire et proportionnel. Par exemple, dans l'affaire *Klass c. Allemagne*, la Cour européenne des droits de l'homme a insisté pour que toute exception au droit à la vie privée, notamment quand la mesure facilite la surveillance des communications des citoyens, devait être interprétée de manière restrictive. Il y est indiqué que « le pouvoir de surveiller en secret les citoyens n'est tolérable d'après la Convention que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques »[170]. De plus, la CJUE a déterminé en 2021 dans l'affaire C-746/18 (*Prokuratuur*) que l'accès à un ensemble de données de trafic ou de localisation aux fins d'enquête criminelle, qui fournit des conclusions précises concernant la vie privée d'une personne, « soit circonscrit à des procédures visant à la lutte contre la criminalité grave ou à la prévention de menaces graves contre la sécurité publique »[171].

B. Participation politique

La menace que les restrictions de la vie privée et de la protection des données font peser sur les institutions démocratiques est liée à la question de la sécurité, comme le montre par exemple le Rapporteur spécial des Nations Unies sur les droits à la liberté de réunion pacifique et d'association[172]. Bennett et Raab ont soutenu que, dans un contexte qui se rapproche beaucoup de la politique publique actuelle, la vie privée est considérée comme un obstacle à franchir, car elle entre en conflit avec des valeurs publiques ou communautaires comme la sécurité nationale ou, actuellement, la santé publique.[173] Toutefois, cet argument ne tient pas compte du fait que la vie privée est elle-même une valeur sociale ou publique qui appuie d'autres objectifs de l'administration publique. Par exemple, de bonnes mesures de protection de la vie privée des électeurs (p. ex., scrutin secret, vote par correspondance, scrutin anticipé, etc.) augmentent le taux de participation et la satisfaction à l'égard du processus, ce qui promeut l'objectif de participation politique[174].

Dans d'autres domaines, il faut y entendre que la commodité et l'efficacité que les entités publiques et privées tirent de la création de grandes bases de données (par exemple, les dossiers médicaux nationaux centralisés) ou de méthodes de surveillance continue (comme la STCF, les technologies de reconnaissance faciale ou le suivi comportemental en ligne) doivent avoir comme pendant les risques d'abus. Des dispositifs de sécurité techniques et réglementaires efficaces peuvent empêcher « l'état des bases de données » de devenir l'équivalent virtuel du « bâtiment panoptique », le célèbre modèle de prison de Jeremy Bentham. En effet, le « regard inégal » qui caractérise ce type de surveillance risque de provoquer l'assimilation d'un état d'esprit disciplinaire chez les personnes observées. Bien que, d'une part, les personnes continuellement observées soient moins susceptibles

d'enfreindre les règles ou les lois, d'autre part, il est possible de les dissuader d'exercer leurs droits et libertés individuels ou de participer en général au processus démocratique. Pour reprendre les mots de Bloustein, [traduction] « la vie privée protège nos désirs individuels contre la pression du conformisme »[175].

De plus, l'utilisation non réprimée des données personnelles par les autorités publiques est aussi susceptible d'avoir d'autres effets négatifs sur la société, notamment sur l'adhésion et la cohésion sociale. Lyon soutient que les moyens automatisés de traitement des données peuvent créer une situation où [traduction] « les êtres humains sont décomposés en flux de données, pour être recomposés en "images de données" dans les bases de données des autorités »[176]. Ces dernières années, il est devenu apparent que si les utilisateurs de données peuvent utiliser ces images de données pour établir le profil de risque, il pourrait alors évoluer vers une forme de « classement social » qui peut privilégier certains citoyens et en désavantager d'autres en les incluant dans des catégories de « personnes soupçonnées » avant même qu'ils aient commis un crime[177]. En d'autres mots, ce qui est au départ un problème de trop grande collecte non ciblée se transforme en une possibilité de discrimination et de mauvais traitement de certaines personnes.

De plus, les systèmes de profilage posent aussi un risque de « reproduire et renforcer les divisions sociales, économiques et culturelles dans les sociétés d'information »[178]. Les mesures qui minent la confiance sociale minent aussi la solidarité sociale par leur approche axée sur le comportement individuel[179]. C'est dans ce contexte que Regan insiste sur l'importance de la protection de la vie privée pour prévenir la division de la sphère publique en encourageant les personnes à y vivre en fonction de leurs points communs plutôt que de leurs différences[180]. Bennett et Raab ajoutent que la catégorisation sociale peut donner lieu à des inégalités en matière de vie privée quand [traduction] « la scène politique publique est mise à mal si la limitation du pouvoir arbitraire ne peut être exercée que par certaines personnes ou catégories, peut-être privilégiées sur le plan de la vie privée »[181]. Le fait que certaines personnes bénéficient de la protection de leur vie privée alors que d'autres n'en bénéficient pas peut faire autant de tort au tissu social que les intrusions dans la vie privée des institutions publiques et privées.

C. Santé publique et autres intérêts publics

La santé publique monopolise l'attention du public depuis quelque temps. Face à la pandémie de COVID-19, de nombreux États ont proposé des interventions fondées sur des données, soulevant des préoccupations, d'un côté, quant à la compatibilité de telles initiatives avec les droits fondamentaux et, d'un autre côté, quant au fait que la protection des droits fondamentaux pourrait nuire à l'efficacité de l'intervention face à la pandémie[182]. Un exemple probant d'intervention axée sur les données a été le déploiement d'applications de « traçage de contacts » dans des pays du monde entier. Ces applications illustrent bien le caractère restreint des droits à la vie privée et à la protection des données, ainsi que le rôle que joue le respect de ces droits pour renforcer la confiance du public[183].

Même s'il pourrait donc être tentant de rejeter ou de limiter l'application de ces droits en période trouble comme une pandémie, l'existence de cadres juridiques qui sont

Applications mobiles de traçage de contacts

Les applications de traçage de contacts détectent toute proximité entre deux appareils mobiles et consignent cette rencontre. Ce journal des contacts peut être conservé sur l'appareil ou sur un serveur centralisé. Si une personne présente des symptômes ou est déclaré positif à la COVID-19, alors ces renseignements peuvent être saisis dans l'application. Le risque que d'autres contacts contractent la maladie est alors calculé sur l'appareil ou un serveur centralisé, et les contacts « à risque » sont avertis. Les applications basées sur le traitement centralisé et décentralisé des données personnelles portent atteinte aux droits à la vie privée et à la protection des données. En revanche, pourvu que ces atteintes soient conformes à la loi et que des mesures de protection pertinentes soient mises en place pour les minimiser, ces applications sont néanmoins jugées compatibles avec ces droits. Par exemple, en Angleterre et au Pays de Galles, l'application initiale proposée par le National Healthcare Service (NHS) et appuyée par le gouvernement permettait de recueillir les détails des rencontres sur un serveur centralisé qui calculait le risque d'infection avant de le communiquer aux personnes concernées. Cette application a défrayé la chronique et acquis une image négative en raison de l'incapacité à définir clairement quels sont les objectifs du traitement centralisé des données, qui auraient accès aux données, et à respecter les mesures de protection des données de base, comme la limitation du stockage. Le respect de ces droits fondamentaux pourrait renforcer la confiance du public envers ces applications et ainsi améliorer leur efficacité globale, car la recherche indique que des taux d'adhésion élevés (d'au moins 60 % de la population) sont essentiels à leur efficacité.

l'expression de ces droits peut être salutaire. En effet, une réglementation très limitée ou inexistante pour protéger ces droits (par exemple, ne s'appliquant qu'aux fournisseurs de soins de santé du secteur public) pourrait ouvrir la voie à toute une série de fournisseurs d'applications de traçage de contacts. Dans le domaine des applications de traçage de contacts, une application fiable et conforme aux droits de la personne est infiniment supérieure à une série d'applications concurrentes de qualité douteuse.

D. Liberté d'expression

On attribue à Internet la désintermédiation du discours : alors que la communication de masse n'était autrefois accessible qu'à des diffuseurs privilégiés, comme les chaînes de télévision, les stations de radio et la presse écrite, toute personne disposant d'un appareil connecté à Internet peut désormais diffuser à l'ensemble de la population. Internet a également remis en question les frontières territoriales traditionnelles, permettant aux personnes et aux groupes de rejoindre de nouveaux publics et de découvrir de nouveaux contenus. Cette évolution est généralement considérée comme positive pour la liberté d'expression et d'information. Par contre, elle a avivé les tensions entre la liberté d'expression et d'information, et les droits à la vie privée et à la protection des données, l'exemple le plus frappant étant l'application du « droit à l'oubli ». Pourtant, l'application du « droit à l'oubli » montre que, si ni la liberté d'expression et d'information, ni la protection des données et de la vie privée ne sont traitées comme des droits absolus, elles peuvent être conciliées d'une manière qui respecte l'essence de tous les droits.

Le droit à l'oubli

Le « droit à l'effacement » prévu par la législation européenne sur la protection des données peut être invoqué par une personne contre un moteur de recherche si son nom est utilisé comme terme de recherche afin que certains liens soient retirés des résultats obtenus. Dans la décision rendue par la CJUE (*Espagne*), la Cour a indiqué qu'un tel retrait, en l'occurrence un retrait d'information concernant une insolvabilité survenue près de vingt ans plus tôt, pouvait se produire quand le traitement des données était incompatible avec la législation sur la protection des données. En pratique, cette décision a obligé la Cour à concilier les droits à la protection des données et à la vie privée de cette personne avec la liberté d'expression et d'information des utilisateurs du moteur de recherche de Google. Ce faisant, la Cour a estimé que, normalement, les droits à la protection des données et à la vie privée l'emportaient sur l'intérêt du public à obtenir cette information, à moins que l'intérêt du public à recevoir cette information soit prévalent. La Cour a indiqué qu'étant donné la nature délicate de l'information pour la personne concernée et que les événements auxquels elle se rapportait s'étaient produits seize ans plus tôt, le lien devait être retiré dans certaines circonstances. La jurisprudence ultérieure au Royaume-Uni et en Allemagne a rajusté la « règle générale » afin de rétablir un meilleur équilibre entre la protection des données et de la vie privée et la liberté d'expression. Si ce rajustement inévitable, le caractère restreint de la décision de la Cour a toujours permis une telle conciliation. Quelques réserves importantes méritent d'être relevées.

- Alors que la décision a abouti à des affirmations selon lesquelles des documents « juridiques » étaient retirés des moteurs de recherche, les documents retirés sont « illégaux », car ils sont incompatibles avec la législation sur la protection des données. Le droit à l'effacement ne permet pas à une personne de faire effacer n'importe quelle information. Le facteur déterminant est la compatibilité avec le cadre juridique et non les préférences des personnes ou si elles ont été lésées par l'information.

- Ce droit n'exige pas que les données personnelles soient retirées du dossier historique. La Cour a fait la distinction entre la publication par le site d'origine et la disponibilité de l'information sur le moteur de recherche de Google, qui touche aux droits fondamentaux à la vie privée et à la protection des données « de manière significative et additionnelle » comparativement aux éditeurs de sites Web (arrêt *Google Espagne*, para 38). Selon cette logique, la publication et la distribution dans différents contextes peuvent avoir une incidence qualitativement différente sur les droits à la protection des données et à la vie privée.

- Ce droit ne s'applique pas quand la personne concernée participe à la vie publique, comme « les hauts fonctionnaires, les gens d'affaires et les membres de professions (réglementées) ». En pratique, les demandes de retrait « tiendront systématiquement compte de l'intérêt du public à avoir accès à l'information. S'il l'emporte sur les droits de la personne concernée, alors le retrait ne sera pas approprié ». En reconnaissant que chaque information qui intéresse le public n'est pas nécessairement d'intérêt public, ces droits peuvent être conciliés dans le respect des principes fondamentaux de chacun.

Il importe aussi de rappeler le rôle de la protection des données et de la vie privée dans la réalisation du droit à la liberté d'expression et d'information. La vie privée est co-constitutive de la liberté d'expression[184] et a été décrite par un ancien rapporteur de l'ONU sur la liberté d'expression [traduction] « comme une passerelle vers la

liberté d'opinion et d'expression »[185]. Richards explique ce rôle de facilitateur avec beaucoup d'éloquence quand il plaide en faveur de notre [traduction] « vie privée intellectuelle », un type de vie privée essentiel non seulement aux intellectuels, mais aussi à chacun de nous[186]. Dans une optique normative, il ajoute que la vie privée intellectuelle est la pierre d'assise de la liberté d'expression. Il reconnaît ainsi que la liberté de pensée et de croyance est nécessaire à l'innovation et pour que les citoyens puissent [traduction] « se faire leur opinion sur des idées, grandes et modestes, politiques et banales »[187]. La vie privée est une condition préalable à ce genre de réflexion.

D'un point de vue empirique, en l'absence de vie privée et sous surveillance (par des acteurs publics ou privés), tout porte à croire que notre liberté de pensée et d'action est touchée. Richards ajoute que [traduction] « toute personne surveillée pendant la pratique d'activités intellectuelles (au sens large : penser, lire, naviguer sur le Web ou communiquer en privé) renoncera à avoir des pensées ou à poser des gestes qui pourraient susciter l'intérêt d'autres personnes »[188]. On voit donc que la vie privée protège les principaux aspects de l'expression, allant du fait de se forger une opinion initiale à sa diffusion ultérieure. Elle crée les conditions environnementales qui permettront à la liberté d'expression de s'épanouir.

Au-delà du besoin de protection de la vie privée intellectuelle, il est possible d'imaginer de nombreuses situations où un refus d'accès à l'information peut constituer une atteinte au droit à la vie privée. Un exemple frappant est l'action intentée par *Open Door et Dublin Well Woman* contre le gouvernement irlandais[189]. Les demandeurs avaient fait l'objet d'une ordonnance leur interdisant de fournir certains renseignements aux femmes enceintes sous forme de conseils non dirigés sur les cliniques d'avortement. Ils ont soutenu que le refus de donner de l'information sur l'avortement à l'étranger constituait une ingérence injustifiable dans leur droit au respect de la vie privée et une atteinte à leur liberté de recevoir ces renseignements[190].

La relation entre la protection de la vie privée et des données et la liberté d'expression et d'information est multidimensionnelle. Lorsque ces droits entrent en conflit, chacun cède du terrain pour satisfaire l'autre, comme c'est le cas pour le droit à l'oubli. Dans d'autres circonstances, ces droits sont les deux côtés d'une même médaille, se complétant et se soutenant mutuellement. Par exemple, l'expérience de nombreux groupes marginalisés montre que leur droit à la libre expression ne peut souvent être protégé et exercé qu'avec un droit réel à la vie privée (p. ex., les adolescents LGBTQ2SI qui vivent avec des adultes homophobes ou transphobes, ou les femmes victimes de violence familiale)[191].

E. Égalité et non-discrimination

À notre époque, l'égalité, la non-discrimination et la protection de la vie privée sont étroitement liées.

Le droit à la vie privée peut permettre à des groupes marginalisés de rechercher une communauté commune sans crainte, de s'organiser et de protester, et de défendre leurs droits à l'égalité[192]. Ce droit peut aussi protéger les enfants et favoriser leur

développement complet et équitable. Il peut permettre aux personnes handicapées de bénéficier de services accessibles et d'être accueillies sans devoir divulguer de renseignements médicaux personnels. Il peut aider les femmes et les personnes LGBTQ2SI à trouver la sécurité, à s'accepter et à chercher à sortir de la violence familiale ou des abus. Il peut les protéger contre le harcèlement en ligne et les crimes haineux dans le monde réel[193].

Le droit à la vie privée peut aussi permettre une réalisation plus importante d'autres droits à l'égalité.

Les nouvelles utilisations de l'IA sont particulièrement préoccupantes chez les gens vulnérables qui peuvent disposer de peu d'information ou de ressources sur la façon de faire valoir leur droit à la protection de la vie privée ou leurs droits de la personne. C'est d'autant plus vrai et alarmant pour les enfants[194] qui, dès leur naissance, sont de plus en plus touchés par les technologies de surveillance[195]. Les Nations Unies[196], les régions[197] et les pays[198] ont des discussions critiques[199] et qui évoluent rapidement sur la gouvernance, la réglementation et l'orientation[200], ainsi que sur l'importance des

Lutter contre la discrimination algorithmique

Dans son rapport intitulé *Closer to the Machine*, le Commissariat victorien à l'information cite plusieurs exemples de formes algorithmiques de discrimination dans les secteurs public et privé, dont l'utilisation par Amazon d'un outil d'embauche expérimental qui numérisait et notait les curriculums vitæ des postulants, et qui favorisait les hommes, car le système d'IA avait été formé au moyen de données provenant surtout de curriculum vitæ d'hommes (p. 29/30). Selon ce rapport (p. 32), nombre de facteurs font obstacle à la compréhension des cas de discrimination algorithmique, dont les suivants :

- La personne concernée peut ne pas savoir que la décision a été prise par un système d'IA;
- L'utilisateur du système d'IA peut ne pas être obligé de donner une explication, surtout dans un contexte commercial;
- Le concepteur du système d'IA peut refuser de révéler son processus de raisonnement pour maintenir ses avantages commerciaux et concurrentiels et préserver le secret;
- La piste d'audit du système d'IA peut ne pas indiquer les facteurs pertinents pour la décision ou la recommandation formulée par le système d'IA.

Le RGPD de l'UE prévoit un droit à l'explication, qui comprend une obligation de communiquer de l'information sur « l'existence d'une prise de décision automatisée, y compris un profilage » et « des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée ». Cette obligation s'applique à la fois à la première collecte de données personnelles ou peu après (alinéas 13(2)f) et 14(2)g) du RGPD) et après le début du traitement des données personnelles (alinéa 15(1)h) du RGPD). Dans le même esprit, la Convention 108 modernisée confère aux personnes, sur demande, le droit de prendre « connaissance du raisonnement qui sous-tend le traitement de données, lorsque les résultats de ce traitement lui sont appliqués » [alinéa 9(1)c)]. Le droit en matière de protection des données permet donc d'éliminer les obstacles qui empêchent de comprendre la discrimination algorithmique et de mettre au jour les pratiques discriminatoires.

droits de la personne dans ces cadres et débats[201]. Les organes de l'ONU[202], les organisations de la société civile[203], les défenseurs des droits de la personne[204], les instituts universitaires et de recherche[205], les commissaires à la protection de la vie privée[206] et les institutions nationales des droits de la personne[207] jouent tous des rôles prépondérants dans ces débats sur la façon d'assurer la pleine protection et l'amélioration adéquate des droits de la personne au fil de l'évolution technologique.

Précisons que, d'un point de vue opérationnel, bien qu'un instrument international ou une constitution nationale comportant des principes d'égalité puissent contraindre les initiatives dans de nombreux États, ils ne permettent pas de rendre des comptes ou d'offrir un recours contre les initiatives des entreprises privées. Les codes nationaux des droits de la personne, qui sont de nature quasi constitutionnelle, forment une importante protection législative supplémentaire. Ils peuvent promouvoir l'égalité et le droit à la vie privée et obliger les secteurs public et privé à rendre des comptes en cas de discrimination. Pour nombre d'États, les institutions nationales des droits de la personne, comme les commissions des droits de la personne, collaborent avec les bureaux nationaux ou régionaux des commissaires à la protection de la vie privée, et ils peuvent appuyer et renforcer leurs travaux réciproques sur l'égalité et la vie privée.

Un autre type de relation entre la protection des données et de la vie privée et le droit à l'égalité s'oriente surtout sur le rôle de la protection des données et de la vie privée dans la dissimulation ou la divulgation de pratiques discriminatoires. On dit parfois que les règles quant au traitement des renseignements personnels de nature délicate nuisent aux efforts de collecte de données visant à évaluer et atténuer la discrimination[208]. Par exemple, Binns et Veale laissent entendre que de nombreuses méthodes de lutte contre la discrimination algorithmique supposent d'entrée de jeu que les organisations détiennent ces données de nature délicate afin de s'assurer du respect du cadre de protection des données, alors que ce n'est peut-être pas le cas[209].

Cependant, les droits à la vie privée et à la protection des données servent le plus souvent à soutenir les efforts de lutte contre la discrimination. En effet, certains des premiers documents internationaux sur la protection des données et de la vie privée (deux résolutions du Conseil de l'Europe sur la protection de la vie privée vis-à-vis des banques de données électroniques) établissent des mesures de protection à appliquer [traduction] « [p]articulièrement lorsque des banques de données électroniques traitent des informations concernant l'intimité de la vie privée des personnes, ou lorsque le traitement des informations peut être à l'origine de discriminations »[210]. De plus, de nombreux cadres modernes de protection des données énoncent un grand principe : le traitement « équitable » des données personnelles, qui signifie notamment « non discriminatoire »[211]. Par exemple, le « Marco Civil da Internet » brésilien énumère la « non-discrimination » et non l'équité parmi les principes généraux du traitement des données personnelles, affirmant que l'assemblée législative brésilienne a estimé que la non-discrimination constituait l'élément le plus important de l'équité à protéger[212]. Il en va de même pour l'autorité française de protection des données qui a conclu dans un récent rapport sur les algorithmes et l'IA qu'un « algorithme loyal ne devrait pas avoir pour effet de susciter, de reproduire ou de renforcer quelque discrimination que ce soit »[213].

7. Prochaines étapes : options pour l'évolution des droits à la vie privée et à la protection des données

L'effort pour accroître la reconnaissance et l'application des droits à la protection des données et à la vie privée est justifié par leur utilité à la fois inhérente et instrumentale pour les personnes et la société. Malgré le lien très clair expliqué ci-dessus entre la protection des données et de la vie privée et d'autres droits, une protection optimale de l'un ou l'autre d'entre eux n'est pas encore assurée. Si de nombreux facteurs contribuent à cette absence de mesures de redressement efficaces, deux d'entre eux méritent d'être soulignés.

Premièrement, comme nous l'avons mentionné ci-dessus, malgré la prolifération des régimes de protection des données dans le monde[214], les distinctions entre les cadres de protection des données et les cadres de protection de la vie privée sont de plus en plus grandes. D'un côté, certains régimes s'appuient sur les droits fondamentaux et défendent les droits des personnes et de la société. D'un autre côté, certains sont plus axés sur le marché et visent avant tout à protéger les intérêts de la libéralisation des données. Les deux modèles ont de fervents partisans. Or, du point de vue des mesures de redressement, plus il y aura de pays qui adoptent le modèle des droits fondamentaux et interprètent leurs cadres réglementaires d'une manière qui favorise la protection des droits, plus cette protection sera efficace.

Deuxièmement, pour les pays qui adoptent une approche de la protection des données personnelles fondée sur les droits fondamentaux, il est important que la loi soit adoptée dans la législation locale, puis appliquée et respectée. Il s'agit notamment d'établir une autorité indépendante chargée de superviser l'exécution de la protection des données et de s'assurer que son travail est appuyé par des ressources suffisantes et exempt de toute ingérence extérieure. Cette réglementation publique devrait aussi être renforcée par des procédures de redressement privé qui reconnaissent et facilitent les actions individuelles en dommages-intérêts et les recours collectifs visant à combler les lacunes collectives et systémiques de la protection de données.

À l'heure actuelle, les instruments existants de protection des données et de la vie privée sont mal appliqués à l'échelle tant nationale qu'internationale. L'absence de réponse à ces problèmes videra la législation sur la protection des données de toute véritable substance, transformant ce qui devrait être un moyen efficace de protéger les droits et de renforcer la confiance et la responsabilité à l'ère numérique en un exercice de cases à cocher qui justifie l'usage impropre ou abusif des données plutôt que de le remettre en question.

Étant donné l'importance d'assurer une protection efficace des données et de la vie privée, il faut alors se demander comment assurer une telle protection des droits. Le principal choix est de savoir s'il faut préconiser de nouveaux instruments juridiques qui reconnaissent explicitement la dimension de droits fondamentaux de la protection des données et de la vie privée, ou s'il faut prôner le renforcement et l'amélioration des protections juridiques nationales et internationales existantes.

Au cours des dernières décennies, de nombreux États européens ont adopté une protection constitutionnelle pour la protection des données dans leurs systèmes

juridiques nationaux. Dernièrement, au Luxembourg, un projet de réforme constitutionnelle prévoit l'inclusion d'un droit à « l'autodétermination informationnelle » dans la Constitution (en plus du droit existant à la vie privée figurant au paragraphe 11(3)). Cette proposition s'inspire explicitement du droit à la protection des données de la Charte de l'UE et de la jurisprudence allemande sur l'autodétermination informationnelle[215]. Bien que cette approche offre l'avantage d'assises juridiques fermes pour les droits à la protection des données et à la vie privée, elle risque aussi de devenir encombrante dans les États où la réforme constitutionnelle exige d'importantes mesures procédurales (comme l'approbation par référendum). La modification des traités à l'échelle internationale pourrait encore se prolonger. Voilà pourquoi il est préférable d'adopter la deuxième approche : le renforcement de la protection juridique nationale et internationale existante. Non seulement il est plus réaliste d'un point de vue pratique d'adopter cette approche, mais celle-cie est aussi plus respectueuse des divers contextes constitutionnels et culturels des États.

A. Mieux exploiter le potentiel de la protection existante à l'échelle nationale

L'approche immédiate et donc pragmatique pour s'assurer que la nature axée sur les droits de la loi sur la protection des données soit généralement reconnue consiste à militer en faveur de la reconnaissance explicite des droits à la protection des données et à la vie privée dans les lois et cadres constitutionnels nationaux, s'il y a lieu. Les cours constitutionnelles et les cours suprêmes nationales ont tendance à pouvoir tirer parti des dispositions constitutionnelles existantes pour reconnaître ces droits. Comme nous l'avons mentionné ci-dessus, c'est la voie empruntée par la Cour constitutionnelle allemande pour définir un droit à l'autodétermination informationnelle axé sur les droits actuels à la dignité humaine et à l'autodétermination de la Loi fondamentale allemande.

C'est aussi l'approche préconisée par la Cour suprême de l'Inde dans l'arrêt *Puttaswamy* en 2017. Dans cet arrêt, la Cour suprême a conclu à l'unanimité que le droit à la vie privée est un droit protégé par la Constitution indienne, bien qu'il n'y soit pas explicitement écrit. Les neuf juges ont rendu six avis distincts, le raisonnement de chacun étant un peu différent. En revanche, ils partageaient un même constat : la protection de la vie privée ne peut être déconnectée des autres droits constitutionnels, comme la liberté, la dignité et la liberté d'expression. Comme l'indique l'arrêt :

> [traduction]
>
> La vie privée n'a pas été présentée comme un droit fondamental indépendant, ce qui n'enlève rien à la protection constitutionnelle dont elle jouit, dès lors que l'on comprend la vraie nature de la vie privée et son lien avec les droits fondamentaux qui sont expressément protégés. La vie privée fait partie de l'ensemble des libertés protégées[216].

Ce raisonnement constitue un exemple prometteur pour le développement des droits à la vie privée et à la protection des données dans d'autres pays. Ce qu'il y a aussi de pertinent dans le jugement principal (du juge DY Chandrachud), c'est qu'outre

son engagement détaillé envers la jurisprudence nationale en matière de vie privée et les droits constitutionnels, il a aussi étudié beaucoup d'autres ressorts, dont la Cour européenne des droits de l'homme et la Cour interaméricaine des droits de l'homme, ainsi que les principaux travaux de recherche sur la vie privée, et s'en est inspiré. Cette synergie des développements jurisprudentiels et des idées pourrait aussi permettre de faciliter la reconnaissance de ces droits dans d'autres pays.

Si elle est autorisée par le système judiciaire national, cette approche a l'avantage de ne nécessiter aucune réforme constitutionnelle ou juridique radicale. Si l'on veut évaluer la viabilité de la promulgation de la vie privée, il faut commencer par examiner le cadre constitutionnel et la jurisprudence et cerner les éléments communs sur lesquels compter pour appuyer le droit à la vie privée ainsi que les pouvoirs des tribunaux pour interpréter et reconnaître les droits fondamentaux. Quand cela est possible, les défenseurs de la protection des données et de la vie privée (organismes de réglementation, organisations internationales comme le Conseil de l'Europe, universitaires et autres intervenants) pourraient collaborer avec des organisations locales pour fournir une expertise et renforcer les capacités et la sensibilisation en matière de protection des données et de la vie privée.

B. Favoriser la convergence vers les instruments internationaux actuels axés sur les droits

Plutôt que de tenter de réaliser un consensus sur un nouvel instrument international de protection des données, il pourrait être préférable d'assurer une convergence vers un instrument international actuel axé sur les droits. Trois options peuvent être envisagées pour choisir l'instrument le plus approprié.

La première pourrait être de favoriser une plus grande convergence sur les principes de protection des données et de la vie privée sous l'égide de la disposition relative à la vie privée du PIRDCP. L'objectif serait notamment d'inciter au respect et à l'application du droit du PIRDCP et de veiller à ce que son interprétation et son application soient adaptées à l'ère numérique. Par exemple, le CDHNU pourrait adopter une nouvelle « observation générale » sur l'article 17 du PIRDCP, tenant compte des intérêts collectifs visés par le droit à la vie privée et modernisant son interprétation de l'article 17.

En revanche, étant donné que les approches de l'ONU à cet égard ont échoué, il est risqué d'emprunter cette voie. Pour commencer, l'ONU compte parmi ses membres des États fortement attachés à des approches envers la protection des données axées sur l'économie et d'autres à des approches axées sur les droits. Il est donc possible que ces diverses perspectives sur le rôle approprié de la protection des données dans un environnement numérique affaiblissent toute protection conférée par l'ONU.

La deuxième option serait de favoriser la convergence vers le RGPD de l'UE comme norme internationale. Les dispositions de fond du RGPD relatives au traitement des données personnelles sont nombreuses et soigneusement détaillées : elles ont été rédigées en sachant que le traitement des données personnelles se répercute sur les droits fondamentaux et doit donc être assujetti à de solides mesures de

protection. De plus, de nombreux États sont déjà au fait de ces normes. Dans certains États, le RGPD a été explicitement ou implicitement pris en compte lors de la rédaction des lois nationales afin de déterminer « l'adéquation » nécessaire pour assurer la circulation transfrontalière des données entre les États membres de l'UE et des pays tiers[217].

Néanmoins, la convergence vers la norme du RGPD n'est peut-être pas l'option la plus attrayante pour plusieurs raisons. Avant tout, étant donné que l'on vante le RGPD comme un « modèle » pour la protection des données et qu'il vise à assurer la poursuite de l'intégration européenne au moyen de dispositions strictes et normatives, il pourrait, dans l'immédiat, être hors de portée comme norme juridique pour de nombreux États. De plus, les seuls signataires non européens du RGPD sont des États de l'Espace économique européen (EEE) [Islande, Liechtenstein et Norvège]. Aucun autre mécanisme n'est prévu pour que les États non membres de l'UE et de l'EEE adhèrent officiellement aux normes du RGPD.

La troisième option, qui est peut-être la plus viable, consiste à favoriser la convergence vers la Convention 108+ du Conseil de l'Europe. Cette Convention « modernise » la version originale par un protocole d'amendement (CETS n° 223). Voici donc les avantages d'appuyer une plus grande convergence internationale par l'intermédiaire de la Convention 108+.

Premièrement, bien que la Convention 108+ n'entre en vigueur qu'en 2023, au plus tôt, les États non européens signataires peuvent déjà demander à y adhérer[218]. Bien que les détails du « mécanisme d'évaluation et de suivi » prévu par la Convention 108+ n'aient pas encore été arrêtés, les demandes d'adhésion à la Convention seront d'abord évaluées par le « Comité conventionnel » qui appréciera l'efficacité des mesures prises par l'État (ou l'organisation internationale) demandeur pour donner effet aux dispositions de la Convention[219]. Après cette évaluation, le Comité conventionnel adopte un avis positif ou négatif sur l'admissibilité de l'État demandeur à l'adhésion qui est transmis au comité des ministres du Conseil de l'Europe[220]. Huit États non membres du Conseil de l'Europe ont déjà ratifié la Convention 108, alors que trois ont signé et un a ratifié la Convention 108+[221]. Les États non européens jouent aussi un rôle d'observateurs au sein du « Comité consultatif » de la Convention 108 (qui sera remplacé par le Comité conventionnel)[222].

Fort avantageusement, la Convention 108+ est déjà conçue comme une norme internationale et multilatérale de protection des données et dispose des procédures applicables à son adhésion[223]. En effet, le Conseil de l'Europe a déclaré qu'il demeure résolu à aider les parties à procéder à :

> [traduction]
>
> *une adhésion rapide au Protocole [CETS no 223] par le plus grand nombre possible d'États actuellement parties à la Convention n° 108 afin de faciliter la création d'un régime juridique global de protection des données en vertu de la Convention modernisée, ainsi que d'assurer la représentation la plus large possible d'États au sein du Comité conventionnel*[224].

Le Conseil de l'Europe dispose déjà d'un modèle pour favoriser l'adoption de ses conventions au-delà des frontières européennes et s'assurer qu'elles prennent une envergure vraiment mondiale. Par exemple, 21 parties non européennes ont ratifié la Convention sur la cybercriminalité[225].

Deuxièmement, les normes énoncées dans la Convention 108+ sont plus strictes que celles de la Convention 108, ce qui garantit que l'instrument est conforme à la dernière génération de lois sur la protection des données. Par contre, ces normes ne sont pas aussi normatives que celles du RGPD de l'UE : elles offrent ainsi un « juste milieu » et une vaste marge de manœuvre pour de nombreux pays. Comme le mentionne Greenleaf, l'adhésion à la Convention 108+ permet notamment aux États de [traduction] « reconnaître les pratiques exemplaires », à savoir que [traduction] « les normes de protection des données d'un pays sont devenues des "pratiques exemplaires internationales" d'après un groupe de plus en plus mondialisé de pairs du pays »[226]. De plus, rien n'empêche les États qui le veulent d'aller plus loin que les normes énoncées dans la Convention 108+ (voir l'article 13 de la Convention 108+). La Convention 108+ pourrait donc être considérée comme une norme mondiale de protection des données « prête à l'emploi » placée au niveau approprié pour une large adhésion.

Un troisième avantage en faveur de la convergence vers la Convention 108+ comme norme mondiale de protection des données, soutenue par les droits fondamentaux, tient du fait que l'incitation à cette convergence existe déjà. La Commission européenne a notamment encouragé l'adhésion de pays non européens à la Convention 108+ comme « le seul instrument multilatéral contraignant dans le domaine de la protection des données » et « encouragera activement l'adoption rapide du texte modernisé pour que l'UE y devienne partie »[227]. De même, le Rapporteur spécial de l'ONU sur le droit à la vie privée a indiqué que les États membres soient invités à ratifier la Convention 108+ « à titre de mesure minimale visant à harmoniser les règles détaillées de protection de la vie privée à l'échelle mondiale »[228].

Ce n'est pas que l'adhésion à la Convention 108+ doive être considérée comme une panacée pour la protection de la vie privée et des données, car elle présente deux grands défis. Le premier concerne les normes de fond. Comme le mentionne Greenleaf, pour de nombreux pays, il est peu probable que certaines des conditions préalables à l'adhésion (notamment être reconnu comme un État et être un État démocratique) soient bientôt remplies[229]. L'adhésion de ces États est donc une perspective irréaliste à court terme. La présence d'une autorité de contrôle indépendante et des règles comprenant le traitement des données dans les secteurs public et privé sont d'autres conditions à l'adhésion. Ces conditions, bien qu'atteignables pour d'autres États, exigeraient des changements juridiques et culturels. Enfin, il n'est pas certain que les organismes de réglementation existants (p. ex., les institutions nationales des droits de la personne), les titulaires de droits ou les défenseurs de la société civile soient plus largement favorables à cette approche. Avant toute réforme importante, il faudrait mener une consultation gouvernementale ouverte avec ces groupes et organismes.

Greenleaf précise quelques moyens qui pourraient faciliter l'adhésion de ceux qui le veulent. Les voici :

- La publication d'un document de politique par le Comité consultatif qui insiste sur les éléments essentiels de l'évaluation de l'adhésion[230];
- La nécessité pour le Comité de la Convention 108+ (qui sera remplacé par le Comité consultatif) et le Comité des ministres d'être souples dans l'application de la norme d'adhésion à la Convention[231];
- L'évaluation des perspectives d'adhésion par des « analystes indépendants ou "non officiels" comme des universitaires » afin de permettre de prioriser les demandes d'adhésion viables et de former une [traduction] « base adéquate pour un débat public sur les perspectives de tels accords internationaux »[232].

En tenant compte de ces recommandations, il est évident que même s'il est actuellement impossible pour tous les États d'atteindre les normes de la Convention 108+, il est possible de faciliter et de simplifier une telle adhésion que le Conseil de l'Europe est disposé à soutenir.

L'autre défi est lié à l'application des normes de la Convention 108+. Le régime en vigueur ne peut que tenir les signataires de la CEDH responsables en cas de non-conformité. En revanche, il est essentiel d'établir un mécanisme simple et non conventionnel sur la base de l'article 17 de la Convention 108+. Cette nouvelle procédure pourrait servir d'instrument précieux pour faire respecter des cas individuels, même dans des contextes transfrontaliers, et serait fondée sur l'obligation pour les autorités de contrôle de collaborer entre elles, notamment a) en s'accordant mutuellement une assistance par l'échange d'informations pertinentes et utiles et en coopérant entre elles […] et b) en coordonnant leurs enquêtes ou interventions, ou en menant des actions conjointes. En revanche, si un État partie allait à l'encontre de la Convention modernisée, l'article 4, paragraphe 3 de la Convention 108+ devrait permettre au Comité de la Convention a) d'évaluer la situation, b) de recommander des mesures à prendre pour se conformer aux dispositions de la Convention et c) d'appliquer des sanctions imposées en vertu de dispositions de la Convention 108+ (comme le paragraphe 1 de l'article 14) ou de la Convention de Vienne sur le droit des traités. Ces mesures pourraient certainement contribuer ou aboutir à une conformité nationale uniforme avec la Convention. Cela dit, elles doivent encore être élaborées et mises en place pour toutes les parties actuelles et futures, ce qui pourrait poser certains problèmes.

Dans l'intervalle, les autres parties et organes de la Convention (Comité consultatif, Secrétariat et Conseil des ministres) pourraient recourir à un mécanisme non contraignant : essayer de faire respecter la Convention par des moyens diplomatiques. Il y a cependant plusieurs autres possibilités. Le premier protocole facultatif au PIDCP a d'ailleurs été ratifié par 115 États membres de l'ONU. Il permet aux personnes qui affirment qu'un signataire du Protocole a violé leurs droits au titre du PIDCP et qui ont épuisé tous les recours internes disponibles de présenter une « communication » au Comité aux fins d'examen[233]. Le CDH peut alors formuler des recommandations non exécutoires à l'État concerné.

On pourrait aussi envisager d'imposer les dispositions de la Convention 108+ par des cadres régionaux des droits de la personne, comme le Système interaméricain des droits de la personne ou la Cour africaine des droits de l'homme et des peuples. Les réseaux de protection des données existants (comme APPA, GPEN, l'AFAPDP

et l’AMVP) pourraient aussi participer plus activement aux mécanismes onusiens (comme le Haut-Commissariat aux droits de l’homme, le Rapporteur spécial sur le droit à la vie privée et divers comités) déjà engagés dans l’analyse et la promotion du droit à la vie privée à l’ère numérique[234].

C. Conclusion

Les éléments de preuve, les tendances, la jurisprudence et les résultats examinés et signalés dans le présent rapport et dans l'examen juridictionnel connexe ont mené aux conclusions de notre groupe de travail de l'AMVP énumérées ci-dessous. Certaines de ces conclusions peuvent sembler évidentes (voire axiomatiques) pour les acteurs du domaine de la réglementation des données ou de la protection des droits, car il s'agit de phénomènes que nous observons depuis plus de vingt ans. Nous les réaffirmons clairement ci-dessous afin de mieux orienter les délibérations et les mesures futures visant à améliorer le statut du droit à la vie privée dans le monde.

1. **Les autres droits civils et politiques des citoyens du monde entier sont menacés sans une protection claire et rigoureuse et une application efficace des droits à la vie privée et à la protection des données.** La liberté de croyance, la liberté de mouvement, la liberté d'association, le droit à la dissidence pacifique, la dignité humaine et l'égalité gravitent tous autour de protections substantielles de la vie privée et de la protection des données. Ces dernières subissent une pression constante des acteurs étatiques et commerciaux. Il est impossible de qualifier d'ouvert, de libre ou d'équitable un monde où personne ne peut échapper à la surveillance des gouvernements et des entreprises.
2. **Toute solution ou réforme proposée pour résoudre les problèmes actuels doit être viable au-delà des frontières nationales et s'appliquer à tous les secteurs d'économies distinctes.** La compartimentation de la réglementation (comme dans les efforts pour mettre un terme à l'injustice fiscale, protéger l'environnement ou améliorer la santé publique) ne font que créer un fossé, des inégalités, des angles morts et des exceptions supplémentaires. Les droits dont on bénéficie dans le monde réel devraient s'appliquer également à notre identité numérique, et les droits à la vie privée que les populations attendent de leurs gouvernements devraient aussi être respectés par les entités commerciales. La libre entreprise ne veut pas dire que tout est permis et le « laissez-faire » ne devrait pas permettre aux entreprises de décider de ce qui est juste. Les dernières décennies ont aussi fait état des vices et des limites de l'autoréglementation de l'industrie et de la nécessité de mesures de protection et de redressement exécutoires pour que les droits soient appliqués.
3. **Les protections qu'accordent les constitutions et les lois locales, les accords bilatéraux ou les conventions et les pactes internationaux doivent faire l'objet d'une analyse, d'un soutien, d'une promotion, d'une éducation et d'une application efficaces dans le monde réel.** Déconnectés de la réalité, les droits de la personne, qui ne permettent aucune mesure de redressement significative ou des mesures trop complexes et coûteuses, n'offrent que des promesses vides. Pour une reddition de comptes réellement efficace, les organismes de surveillance doivent pouvoir compter sur des ressources adéquates, être exempts d'ingérence politique, dotés du personnel voulu et être en mesure de coopérer à l'échelle locale et nationale avec les titulaires de droits et leurs défenseurs, et, à l'échelle mondiale, avec leurs pairs, les Institutions nationales des droits de l'homme, les organismes publics, les organisations régionales et internationales et les mécanismes de l'ONU. Ces principes s'appliquent aussi à la réglementation du gouvernement et du commerce, ainsi qu'aux instruments multilatéraux existants adoptés par l'OCDE, l'UE, le Conseil de

l'Europe et l'APEC. Sans une application significative et proactive, les règles révisées, les normes rééditées et les nouveaux protocoles ne seront ni respectés ni crédibles.

4. **Les atteintes à la vie privée et à la protection des données englobent des préjudices qui dépassent largement la perte de données personnelles.** Les efforts de l'industrie en vue de limiter les discussions sur le traitement de l'information et les mesures de protection des systèmes minimisent sérieusement les dommages subis par les personnes et les communautés. Ces mauvaises pratiques en matière de données, une application inégale, l'exceptionnalisme juridique, l'emprise réglementaire ou le retard constant des efforts déployés pour réformer minent gravement l'autonomie personnelle, la dignité personnelle fondamentale, la liberté de conscience et le droit inaliénable à l'autodétermination individuelle (véritable choix).
5. **Il faut rappeler aux gouvernements la protection de la vie privée et la protection des données et la place centrale qu'elles occupent dans les fondements de la démocratie.** La protection de la vie privée et la protection des données ne sont pas des règles de savoir-vivre, une nouveauté mondaine ou une observation originale de la bonne société. Elles sont le fondement de l'équité électorale (p. ex., le vote secret), des communications privées (p. ex., exigences de mandat) et de l'application courante de la loi (p. ex., le droit d'accéder aux renseignements détenus par le gouvernement, de les examiner et de les corriger).
6. **Les législateurs, les élus, les membres de l'appareil judiciaire et les responsables désignés des organismes de réglementation jouent tous un rôle dans la réforme et le renforcement des institutions de protection des droits.** Les droits fondamentaux ne sont pas des libertés que nous externalisons ou laissons aux marchés et à leurs orientations. Si bien qu'il faut maximiser les effets de l'application locale (p. ex., des arbitres plus compétents et un meilleur accès aux procédures de redressement) tout en faisant de la coopération internationale une grande priorité pour les organismes gouvernementaux (p. ex., élargir les efforts de l'OCDE, de la Convention 108+ et du RGPD).

Le renforcement de la protection des données et de la vie privée et des droits de la personne exigera un engagement soutenu de moyens tangibles et une clarification de nos objectifs. Comme nous l'avons précisé dans le présent rapport, tout indique que l'érosion de la vie privée, de la dignité humaine, de la liberté essentielle et de la liberté d'expression se poursuivra sans une coordination immédiate. L'autre option, une fragmentation persistante des efforts de réforme, des efforts localisés et sporadiques de réglementation, et des ingérences inégales et prolongées dans la mise en application en ligne, confirme le statu quo de l'autoréglementation dans les secteurs commercial et gouvernemental.

Pour être clair, les options présentées dans ce rapport ne sont pas contradictoires, mais complémentaires. Par exemple, bien que la priorité accordée à des instruments comme la Convention 108 et 108+ constitue une voie d'amélioration rapide, il faut aussi que les appels à d'autres mesures internationales (p. ex., en ce qui concerne les Nations Unies) se poursuivent. On peut imaginer deux façons de renforcer et assurer la reconnaissance et la protection des droits à la vie privée et à la protection des données. La première s'inspire des dispositions constitutionnelles existantes, dont

les droits à l'autonomie, à la liberté, à la personnalité et à la dignité, pour reconnaître un droit à la vie privée et à la protection des données dans l'ordre juridique interne d'un État. En l'absence de dispositions explicites en matière de protection de la vie privée ou de protection des données, un certain nombre d'États, dont l'Allemagne et l'Inde, ont déjà utilisé ce moyen. Les retombées ont été importantes.

La deuxième voie, possiblement cumulative, consiste à favoriser la convergence vers un instrument mondial existant fondé sur les droits. Le premier candidat est la Convention 108+. Cette convention a été mise à jour pour en assurer la conformité avec la dernière génération de lois sur la protection des données. De façon générale, il s'agit d'un instrument rigoureux axé sur les droits, mais ses dispositions ne sont pas normatives, ce qui laisse une certaine marge de manœuvre dans des contextes juridiques et culturels différents. Enfin, il existe un processus clair pour l'adhésion des États non membres du Conseil de l'Europe.

Si cette méthode est suivie et que le potentiel des instruments juridiques existants pour la protection de la vie privée est maximisé, une approche fondée sur les droits plus efficace restera alors accessible.

Annexe : Facteurs liés à l'autonomie – intérêt personnel, dépendance économique, relations et obligations sociales

1. Intérêt personnel existentiel

Il est permis de croire que les contraintes liées à l'intérêt personnel existentiel représentent les limites à notre autonomie individuelle les mieux définies. Nous consentons souvent de plein gré à l'utilisation de nos données, s'il s'agit d'une condition préalable pour recevoir certains traitements médicaux ou si la collecte continue de données fait partie du fonctionnement d'un dispositif médical novateur, comme un implant cochléaire ou un stimulateur cardiaque. Le refus de consentir au traitement de nos données, s'il mettait réellement en danger notre santé, notre vie, ou la santé ou la vie d'autrui, peut sembler, à première vue, être vain et ne pas être considéré comme une contrainte. En revanche, cela suppose que le déploiement efficace de mesures de santé individuelles ou publiques est conditionnel au traitement de données personnelles identifiables et qu'il ne peut se faire autrement.

C'est ce qu'on constate dans certains cas. Toutefois, dans d'autres, il peut être tout à fait suffisant de recueillir des données sous forme anonyme. Un droit effectif à la protection des données protégerait l'autonomie individuelle en laissant aux innovateurs la responsabilité de développer de nouvelles technologies selon les principes établis de protection des données, comme la minimisation des données, le principe de finalité et la limitation de la conservation.

2. Contraintes économiques

Les contraintes économiques qui influencent nos choix sont surtout le résultat de notre pouvoir de négociation relatif lors d'interactions avec d'autres acteurs commerciaux. Dans ce contexte, notre pouvoir relatif est notamment déterminé par notre richesse, nos connaissances, nos compétences et nos capacités. En pratique, il s'agit de choses que nous ne pouvons pas faire, que nous ne savons pas faire ou que nous ne pouvons pas nous permettre de faire.

On observe souvent des contraintes économiques dans des contextes où une personne se trouve en situation de dépendance économique ou si elle est prête à faire certains compromis en matière de vie privée en échange de biens ou de services. La relation employeur-employé ou bénéficiaire de prestations-autorité publique qui fournit ces prestations sont des exemples du premier contexte, où il sera quasi impossible pour une personne de refuser une demande de divulgation de ses données personnelles sans risquer de subir un préjudice financier considérable. Les compromis entre les fournisseurs et les utilisateurs de services de réseaux sociaux « gratuits » relèvent de la deuxième catégorie. Les utilisateurs se sont habitués à « payer avec leurs données », non seulement parce qu'ils aiment recevoir des services sans devoir fournir une compensation monétaire, mais aussi parce qu'un nombre important d'utilisateurs ne pourraient se permettre d'utiliser tous ces services s'ils étaient payants. L'utilisation de données comme forme de paiement dissimule une inquiétude plus fondamentale soulevée par notre économie numérique financée par les données et la publicité, en l'occurrence le fait que la compensation monétaire ramènerait l'inégalité économique, qui est manifestement

une caractéristique et non un dysfonctionnement de l'économie politique capitaliste dominante.

On peut aussi observer des contraintes économiques dans d'autres situations, notamment lorsqu'une personne se trouve en situation de dépendance économique. Il s'agit notamment de la relation entre employeur-employé, mais elles peuvent aussi se manifester dans d'autres relations. Par exemple, dans notre monde axé sur la technologie et les données, les personnes tributaires des prestations de l'État (personnes à faible revenu, chômeurs et personnes handicapées) doivent souvent fournir une très grande quantité de données sur leur situation personnelle, leur éducation, leur santé, etc., avant qu'une décision concernant le versement de ces prestations ne soit prise.

Dans ces conditions, les personnes communiqueront à coup sûr leurs données, leur refus risquant littéralement de les laisser sans le sou. Avec de l'argent, nous pouvons acheter le nécessaire pour répondre aux besoins les plus fondamentaux de la hiérarchie de Maslow, comme la nourriture et le logement. Pour le citoyen moyen, ces besoins physiologiques et ces besoins de sécurité sont toujours susceptibles de l'emporter sur des besoins de plus haut niveau comme le développement personnel, dont la capacité d'exercer un contrôle sur nos données personnelles. En revanche, affirmer qu'une personne exerce son autonomie dans ces circonstances reviendrait à faire complètement abstraction du rapport d'inégalité ainsi que du simple besoin économique qui influencera la décision des personnes dans ces circonstances. Au contraire, les inégalités politiques et économiques préexistantes sont susceptibles d'être une contrainte efficace à l'exercice de l'autonomie individuelle dans l'économie des données.

Comme précédemment, le droit à la protection des données peut permettre de réduire ces inégalités et de rétablir un sentiment de véritable autonomie en imposant des restrictions sur des utilisations particulières des données proposées par certains contrôleurs. Bien que, de prime abord, toute restriction de ce type limiterait aussi indubitablement l'autonomie à faire un mauvais marché, dans certains cas, une contrainte sur l'autonomie peut être nécessaire justement pour préserver cette autonomie.

3. Contraintes sociales/collectives

Enfin, nos décisions individuelles sont aussi influencées par les contraintes sociales et collectives, à savoir ce que nous ferons ou non pour remplir nos obligations sociales. Un exemple très actuel de ce type de contrainte est notre volonté de permettre que nos données soient utilisées dans l'intérêt public, notamment en réponse aux appels aux « dons de données » aux fins de santé publique.

Bien que l'intérêt personnel existentiel joue un rôle pour convaincre une personne à participer à de telles mesures de santé publique, une pression « sociale » croissante est aussi exercée pour qu'elle y participe. Il y a des contraintes supplémentaires sur l'autonomie des personnes pour décider de divulguer ou non leurs données à ces fins. Les contraintes sociales et collectives rendent difficile le refus du consentement, et donc le véritable exercice de l'autonomie, malgré les craintes d'un manque de

confiance ou de la possibilité que les données, une fois diffusées, soient utilisées à d'autres fins.

Les lois sur la protection des données ancrées dans la notion d'autonomie individuelle pourraient répondre à certaines de ces préoccupations en limitant les utilisations non essentielles et en exigeant des mesures de protection efficaces. Comme auparavant, la transparence, la minimisation des données, le principe de finalité et la limitation de la durée de conservation des données pourraient contribuer à susciter la confiance requise pour participer à des programmes de traitement de données altruistes ou à valeur sociale sans craindre de subir des préjudices futurs.

En parallèle, dans cette situation particulière, la tension entre les intérêts individuels et collectifs souligne aussi qu'il est peut-être temps de repenser l'individualisme qui a traditionnellement éclairé le concept des droits fondamentaux dans les démocraties libérales occidentales. Comme l'a souligné la Cour constitutionnelle allemande dans sa décision relative au recensement, les actions (ou inactions) des personnes peuvent non seulement avoir une incidence sur elles-mêmes, mais aussi sur les droits et intérêts des autres et de leur communauté. Ainsi, nous devons également nous demander si les droits à la vie privée et à la protection des données doivent être considérés comme des droits purement individuels ou comme des droits collectifs ou communautaires.

Bibliographie/sources citées

Articles

Bloustein, « Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser » (1964) 39 *New York University Law Review* 1000

Bradford et al., « COVID-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR, and Data Protection Regimes » (2020)7 *Journal of Law and the Biosciences* (en attente d'être publié)

Brandeis, L. D. et S. D. Warren, « The Right to Privacy » *Harvard Law Review*, vol. 4, nº 5. (15 déc. 1890), pp. 193-220. - http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C

Crawford et Schultz, « Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms » (2014) 55 *Boston College Law Review* 93

de Hert et Papakonstantinou, « Three Scenarios For International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency » (2013) 9 *Journal of Law and Policy* 271

de Schutter et Ringelheim, « Ethnic Profiling: A Rising Challenge for European Human Rights Law » (2008)71 *Modern Law Review* 358

Diggelmann et Cleis, « How the Right to Privacy Became a Human Right » (2014) 14 *Human Rights Law Review* 441

Ess, « Lost in Translation?: Intercultural Dialogues on Privacy and Information Ethics (Introduction to Special Issue on Privacy and Data Privacy Protection in Asia) » (2005) 7 *Ethics and Information Technology* 1.

Fried, « Privacy » (1968) 77(3) *Yale Law Journal* 475

Greenleaf, « Balancing Globalisation's Benefits and Commitments: Accession to Data Protection Convention 108 by Countries Outside Europe » (2016) *UNSWLRS* 52

Greenleaf, « How Far Can Convention 108+ "Globalise"? Prospects for Asian Accessions » (2020) *Computer Law & Security Review* (en attente d'être publié)

Hoofnagle, van der Sloot et Borgesius, « The European Union General Data Protection Regulation: What It Is and What It Means » (2019) 28 *Information & Communications Technology Law* 65

Keats Citron et Pasquale, « The Scored Society: Due Process for Automated Predictions » (2014) 89 *Washington Law Review* 1

Kitiyadisai, « Privacy Rights and Protection: Foreign Values in the Modern Thai Context » (2005)7 *Ethics and Information technology* 17

Kuner, « An International Legal Framework for Data Protection: Issues and Prospects » (2009)25 *Computer Law and Security Review* 307

Lynskey, « Deconstructing Data Protection: The ”Added-Value” of a Right to Data Protection in the EU Legal Order » (2014) *International & Comparative Law Quarterly* 569

Madison, *Federalist Papers, No. 51* (1788) - https://billofrightsinstitute.org/primary-sources/federalist-no-51

McStay, « Emotional AI, Soft Biometrics and the Surveillance of Emotional Life: An Unusual Consensus on Privacy », janvier 2020, *Big Data & Society* 1

Newman, « The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google » (2014) 40(2) *William Mitchell Law Review* 849

Ohm, « Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization » (2010) 57 *UCLA Law Review* 1701

Olinger, Britz et Olivier « Western Privacy and/or Ubuntu? Some Critical Comments on the Influences in the Forthcoming Data Privacy Bill in South Africa » (2007) 39 *The International Information & Library Review* 31

Petkova, « Privacy as Europe’s First Amendment » (2019) 25 *European Law Journal* 140

Post, « Data Privacy and Dignitary Privacy: Google Spain, the Right to be Forgotten, and the Construction of the Public Sphere » (2018) 67 *Duke Law Journal* 980

Prins, « When Personal Data, Behavior and Virtual Identities Become a Commodity: Would a Property Rights Approach Matter » (2006) 3 *SCRIPTed* 270.

Prosser, « Privacy » (1960) *California Law Review* 48

Rengel, « Privacy as an International Human Right and the Right to Obscurity in Cyberspace » (2014) *Groningen Journal of International Law* 33

Richards, « The Dangers of Surveillance » (2013) 126 *Harvard Law Review* 1934

Simitis, « Die informationelle Selbstbestimmung—Grundbedingung einer verfassungskonformen Informationsordnung » (1984) *Neue Juristische Wochenschrift* 394

Simitis, « Reviewing Privacy in an Information Society » (1987) 135 *University of Pennsylvania Law Review* 709

Spina, « Risk Regulation of Big Data: Has the Time Arrived for a Paradigm Shift in EU Data Protection Law? » (2014) 2 *European Journal of Risk Regulation* 248

Veale et Binns, « Fairer Machine Learning in the Real World: Mitigating Discrimination Without Collecting Sensitive Data » (2017) 4 *Big Data & Society* 1

Veil, « The GDPR: The Emperor's New Clothes - On the Structural Shortcomings of Both the Old and the New Data Protection Law » (2018). Accessible à l'adresse : https://ssrn.com/abstract=3305056

Yilma, « The United Nations Data Privacy System and its Limits » (2019) 33 *International Review of Law, Computers & Technology* 224

Warren et LD Brandeis, « The Right to Privacy » (1890) 4 *Harvard Law Review* 193

Livres

Acemoglu et Robinson, *The Narrow Corridor: States, Societies and the Fate of Liberty* (Penguin Random House, 2019)

Andrejevic, *iSpy: Surveillance and Power in the Interactive Era* (University Press of Kansas, 2007)

Bennett et Raab, *The Governance of Privacy* (2e éd., MIT Press, 2006)

Cohen, J. E., *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press, 2019)

Cohen, S. A. *Invasion of Privacy: Police and Electronic Surveillance* (Carswell, 1983)

Cooley, *A Treatise on the Law of Torts, Or the Wrongs Which Arise Independent of Contract,* (2e éd., Chicago, Callaghan & Company, 1880)

Donohue, *The Future of Foreign Intelligence: Privacy and Surveillance in the Digital Age* (Oxford University Press, 2016)

Emerson, *The System of Freedom of Expression* (Random House Trade, 1970)

Foucault, *Discipline & Punish: The Birth of the Prison* (Vintage, éd. 1995, 1975)

Gonzalez-Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer, 2004)

Hijmans, *The European Union as Guardian of Internet Privacy* (Springer, 2016)

Kant, *Fondements de la métaphysique des mœurs*, (traduction de Victor Delbos, Éditions Les Échos du Maquis, 2013).

Pariser, *The Filter Bubble: What The Internet Is Hiding from You* (Penguin Books, 2011)

Landau, *Surveillance or Security? The Risks Posed by New Wiretapping Technologies* (MIT Press, 2010)

Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press, 2015)

Lyon, *Surveillance After September 11* (Polity Press, 2003)

Lyon, *The Electronic Eye: The Rise of Surveillance Society* (University of Minnesota Press, 1994)

Mayer-Schönberger et Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (John Murray, 2018).

McStay, *Emotional AI* (Sage, 2018)

Raz, *The Morality of Freedom* (Oxford University Press, 1986)

Regan, *Legislating Privacy: Technology, Social Values and Public Policy* (University of North Carolina Press, 1995)

Schoeman, *Privacy and Social Freedom* (Cambridge University Press, 1992)

Shattuck, *Rights of Privacy* (American Civil Liberties Union, 1977)

Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York University Press, 2004)

Solove, *Understanding Privacy* (Harvard University Press, 2008)

Westin, *Privacy and Freedom* (Atheneum, 1967)

Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books, 2019)Zuiderveen Borgesius, *Improving Privacy Protection in the Area of Behavioural Targeting* (Kluwer Law International, 2015)

Chapitres de livres

Andrade, « Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights » in Fischer-Hübner et coll. (dir.), *Privacy and Identity Management for Life* (Springer, 2010)

Dalla Corte, « A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection » in Hallinan et coll. (dir.), *Data Protection and Privacy: Data Protection and Democracy* (Hart, 2020)

de Hert et Gutwirth, « Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action » in Gutwirth et coll. (dir.), *Reinventing Data Protection?* (Springer, 2009)

de Hert et Gutwirth, « Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power » in Claes et coll. (dir.), *Privacy and the Criminal Law* (Intersentia, 2006)

Larsen, Boulanger et Vandendriessche, « Luxembourg » in *The New EU Data Protection Regime: Setting Global Standards for the Rights to Personal Data Protection* (The Hague, 2020)

Oguru, « Electronic Government and Surveillance-Oriented Societies » in D. Lyon (dir.), *Theorizing Surveillance: the Panopicton and Beyond* (Routledge, 2006)

Rauhofer, « Round and Round the Garden?: Big Data, Small Government and the Balance of Power in the Information Age » in Schweighofer et coll. (dir.), *Transparenz* (Oesterreichische Computer Gesellschaft, 2014)

Rouvroy et Poullet, « The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy » in Gutwirth et coll. (dir.), *Reinventing Data Protection?* (Springer, 2009)

W Webster, « Public Administration as Surveillance » in Ball, Haggerty et Lyon (dir.), *Routledge Handbook of Surveillance Studies* (Routledge, 2012)

Jurisprudence

Amann c. Suisse, requête n° 27798/95 (CEDH, 16 février 2000)

Big Brother Watch et autres c. Royaume-Uni, requêtes n^{os} 58170/13, 62322/14 et 24960/15 (CEDH, 4 février 2019)

Botta c. Italie, requête n° 21439/93 (CEDH, 24 février 1998)

Burghartz c. Suisse, requête n° 16213/90 (CEDH, 22 février 1994)

Campbell c. Mirror News Group (MGN) [2004] UKHL 22

Carpenter c. États-Unis 138 S. Ct. 2206 (2018)

Copland c. Royaume-Uni, requête n° 62617/00 (CEDH, 3 juillet 2007)

Digital Rights Ireland Ltd c. Minister for Communications, Marine and Nat. Res. et autres et Karntner Ladesregierung et autres (affaires jointes C-293/12 et C-594/12) [2014] ECR 238

Douglas c. Hello! Ltd [2005] EWCA Civ 595

Fontevecchia et D'Amico c. Argentine, jugement du 29 novembre 2011, Cour interaméricaine des droits de l'homme, (Merits, Reparations and Costs, Series C No. 238)

French Data Network et autres (affaires jointes C-511/18, C-512/18, C-520/18) ECLI:EU:C:020:791

Halford c. Royaume-Uni, requête n° 20605/92 (CEDH, 25 juin 1997)

Justice K.S.Puttaswamy (Retired). c. Union of India And Ors., 2017

Katz c. États-Unis, 389 U.S. 347 (1967)

Kaye c *Robertson* [1991] FSR 62

Kennedy c. Royaume-Uni, requête n° 26839/05 (CEDH, 18 août 2010)

Klass c. Allemagne (1978), requête n° 5029/71 (EHRR, 1978)

La Quadrature du Net et autres (C-511/18) ECLI: EU:C:2020:791

Leander c. Suède, requête n° 9248/81, (EHRR, 26 mars 1987)

Liberty et autres c. Royaume-Uni, requête n° 58243/00 (CEDH, 1er octobre 2008)

Malone c. Royaume-Uni, requête n° 8691/79 (CEDH, 2 août 1984)

Mosley c. News Group Newspapers [2008] EWHC 1777 (QB)

Murray c. Big Pictures (UK) Ltd, [2008] EWCA Civ 446

Niemietz c. Allemagne, requête n° 13710/88 (CEDH, 16 décembre 1992)

Olmstead c. É.-U. (277) U.S. 438 (1928)

Open Door et Dublin Well Woman c. Irlande, requête n° 14235/88 (CEDH, 29 octobre 1992)

Ordre des barreaux francophones et germanophone et autres (affaires jointes C-511/18, C-512/18, 52/18) ECLI:EU:C:2020:7

Privacy International c. Secretary of State for Foreign and Commonwealth Affairs et autres (C-623/17) ECLI:EU:C:2020:790

Rotaru c. Roumanie, requête n° 28341/95 (CEDH, 4 mai 2000)

Schüssel c. Austria, requête n° 42409/98, (CEDH, 21 février 2002)

Smith c. Maryland, 442 U.S. 735 (1979)

Tele2 Sverige AB c. Post-och telestyrelsen et Secretary of State for the Home Department c. Tom Watson et autres (affaires jointes C-203/15 et C-698/15) ECLI:EU:C:2016:970

États-Unis c. Jones, 565 U.S. 400 (2012)

États-Unis c. Miller, 425 U.S. 435 (1976)

Volker und Markus Schecke et Eifert (affaires jointes C-92/09 et 93/09) EU:C:2010:662

Von Hannover c. Allemagne, requête n° 59320/00 (CEDH, 24 septembre 2004)

Weber et Saravia c. Allemagne, requête n° 54934/00 (CEDH, 29 juin 2006)

Zhu Yingguang c. Lianyungang City Branch of China United Network Communications Co., Ltd, Intermediate Court of Lianyungang City, Jiangsu Province, n° 0006 de 2014

Législation et instruments internationaux

Convention américaine relative aux droits de l'Homme, adoptée à la Conférence spécialisée interaméricaine sur les droits de l'Homme, San José, Costa Rica, 22 novembre 1969

Autriche, BGBl. Nr. 59/1964, 1958

Bundesgesetz über den Schutz personenbezogener Daten BGBl 565/1978 (AT)

BVerfGE 35, 202 – Lebach et BVerfGE 65, 1 – Loi relative au recensement

Loi relative au recensement, BVerfGE 65 2020 (DE)

Convention 108+ Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel, ETS n° 108, 1er octobre 1985

Directive 95/46/CE du Parlement européen et du Conseil, du 14 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données [1995] JO nº L 281/31.

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, JO nº L 119/1.

Datenschutzgesetz, 7 octobre 1970 (HDSG)

Dispõe sobre a proteção de dados pessoais e altera a Lei no 12.965, de 23 de abril de 2014 (Marco Civil da Internet), 2014

Union européenne, Charte des droits fondamentaux de l'Union européenne [2012] JO C 326/02

Principes généraux de droit civil 《民法通则 1987

Loi fédérale allemande sur la protection des données de 1977

Conférence internationale américaine, Déclaration américaine des droits et devoirs fondamentaux de l'homme, 9e conférence, Doc. de l'ONU E/CN.4/122 (1948)

Loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques 1979 (LU)

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés 1978 (FR)

Lov nr 294 af 8 juni 1978 om offentlige myndigheders register (DK)

Lov om personregistre mm av 9 juni 1978 nr 48 (NO)

Constitution du Japon *Nihon-koku kenpō*, 1947

Constitution de la Belgique, 1831

The Bermuda Constitution Order, 1968

Loi de 1982 sur le Canada (R.-U.)

Charte canadienne des droits et libertés, 1982

Constitution de la Colombie, 1991

Constitution de la République gabonaise, 1991

Constitution de la République de Corée, 1987

Constitution de Trinité-et-Tobago, 1976

The Datalagen in Sweden in 1973 (Datalagen, 11 mai 1973)

Loi fondamentale de Hong Kong, 1982

The Human Rights Act 1998

Constitution du Mexique, 1917

Constitution des Philippines, 1987

Constitution du Portugal, 1976

Constitution fédérale de la Confédération suisse, 1999

Tort Liability Law (《侵权责任法), 2010

Writ Petition (Civil) No. 494 of 2012, 2017

Rapports et résolutions

Assemblée mondiale pour la protection de la vie privée, « Résolution internationale sur la protection de la vie privée en tant que droit humain fondamental et condition préalable à l'exercice d'autres droits fondamentaux » (octobre 2019) - https://globalprivacyassembly.org/wp-content/uploads/2019/10/Resolution-on-privacy-as-a-fundamental-human-right-and-precondition-for-democracy-2019-FINAL-FR.pdf

The Citizen Lab and Canadian Internet Policy & Public Interest Clinic, « Shining a Light on the Encryption Debate » (mai 2018). Accessible à l'adresse : https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf

Global Commission on Internet Governance, « One Internet » (juin 2016). Accessible à l'adresse : https://www.cigionline.org/sites/default/files/gcig_final_report_-_with_cover.pdf

Conférence internationale des Commissaires à la protection des renseignements personnels et de la vie privée, « Dans un monde globalisé, un droit universel à la protection des données personnelles et à la vie privée dans le respect des diversités » (2005). Accessible à l'adresse : http://globalprivacyassembly.org/wp-content/uploads/2015/02/Montreal-Declaration-French.pdf

Conférence internationale des Commissaires à la protection des renseignements personnels et de la vie privée, « Résolution sur l'inscription de la protection des données et de la protection de la vie privée dans le droit international » (2013). Accessible à l'adresse : https://globalprivacyassembly.org/wp-content/uploads/2015/02/International-Law-resolution-FR.pdf

Commission du droit international, « Rapport de la Commission à l'Assemblée générale sur les travaux de sa cinquante-huitième session » (2006), A 61/10, Annexe D. Accessible à l'adresse : https://legal.un.org/ilc/reports/2006/french/annexes.pdf

The Law Society of England and Wales, « Algorithms in the Criminal Justice System » (juin 2019). Accessible à l'adresse : https://www.lawsociety.org.uk/topics/research/algorithm-use-in-the-criminal-justice-system-report

Rapporteur spécial de l'ONU sur la promotion et la protection du droit à la liberté d'opinion et d'expression, « Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression », Conseil des droits de l'homme, Vingt-neuvième session, point 3 de l'ordre du jour (22 mai 2015). Accessible à l'adresse : https://www.undocs.org/fr/A/HRC/29/32

Rapporteur spécial de l'ONU sur le droit à la vie privée, « Rapport du Rapporteur spécial sur le droit à la vie privée », Soixante-treizième session de l'Assemblée générale de l'ONU (17 octobre 2018). Accessible à l'adresse : https://undocs.org/fr/A/73/438

Rapporteur spécial de l'ONU sur la promotion et la protection du droit à la liberté d'opinion et d'expression, « Rapport au Conseil des droits de l'homme sur la Surveillance et droits de l'homme » (28 mai 2019). Accessible à l'adresse : https://undocs.org/fr/A/HRC/41/35

Autres

Agencia Espanola de Proteccion de Datos, « Draft Joint Proposal for International Standards for the Protection of Privacy and Personal Data » (ébauche non publiée, janvier 2009; ébauche mise à jour les 24 février et 24 avril 2009)

Bedingfield, « Everything That Went Wrong with the Botched A-Levels Algorithm », Wired (19 août 2020). Accessible à l'adresse : https://www.wired.co.uk/article/alevel-exam-algorithm.

Clifford, *The Legal Limits to the Monetisation of Online Emotions* (2019, thèse de doctorat, KU Leuven). Accessible à l'adresse : https://www.law.kuleuven.be/citip/en/research/phd-research/finalized/phd-damian-clifford.

CNIL, « Comment permettre à l'Homme de garder la main? Les enjeux éthiques des algorithmes et de l'intelligence artificielle » (2017). Accessible à l'adresse : https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf

Coughlan, « A-Levels and GCSEs: Boris Johnson Blames "Mutant Algorithm" for Exam Fiasco », BBC (26 août 2020). Accessible à l'adresse : https://www.bbc.co.uk/news/education-53923279.

Commission européenne pour la démocratie par le droit (Commission de Venise), « Luxembourg – Proposition de révision portant instauration d'une nouvelle constitution » (Strasbourg, 27 février 2019) (Rapport du Luxembourg, CDL-REF(2019)006)

deNisco Rayome, « The US, China and the AI Arms Race: Cutting Through the Hype », CNet (8 juillet 2020). Accessible à l'adresse : https://www.cnet.com/news/the-us-china-and-the-ai-arms-race-cutting-through-the-hype/.

de Terwangne, « Convention 108+ Evaluation and Follow-up Mechanisms », 1er juillet 2020. Accessible à l'adresse : https://www.coe.int/en/web/data-protection/follow-up-and-evaluation-mechanism

Commission européenne, « Communication de la Commission au Parlement européen et au Conseil – Échange et protection de données à caractère personnel à l'ère de la mondialisation », COM(2017) 7 final

Gonzalez-Fuster et Hijmans, « The EU Rights to Privacy and Personal Data Protection: 20 Years in 10 Questions », Discussion Paper, Brussels Privacy Hub

Google, « Updating our Privacy Policies and Terms of Service » (24 janvier 2012). Accessible à l'adresse : http://googleblog.blogspot.co.uk/2012/01/updating-our-privacy-policies-and-terms.html

Kuner, « Extraterritoriality and Fundamental Right to Data Protection » (EJIL: Talk, 16 décembre 2013). Accessible à l'adresse : https://www.ejiltalk.org/extraterritoriality-and-the-fundamental-right-to-data-protection/comment-page-1/.

Levin, « Facebook Told Advertisers It Can Identify Teens Feeling "Insecure" and "Worthless" », *The Guardian* (1er mai 2017). Accessible à l'adresse : https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens.

Malgieri, « The Concept of Fairness in the GDPR: A Linguistic and Contextual Interpretation », FAT* '20: Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (ACM, 2020).

Sitaropoulos, « States are Bound to Consider the UN Human Rights Committee's Views in Good Faith » (OxHRH Blog, 11 mars 2015). Accessible à l'adresse : https://ohrh.law.ox.ac.uk/states-are-bound-to-consider-the-un-human-rights-committees-views-in-good-faith/

Comité des droits de l'homme de l'ONU, « Observation générale 16 » (23 mars 1988) (Doc. de l'ONU A/43/40, p. 187–189).

UN, « Guidelines for the Regulation of Computerized Personal Data Files », Rapport final présenté par Louis Joinet, Rapporteur spécial (21 juillet 1988) (E/CN.4/Sub.2/1988/22).

Assemblé générale de l'ONU, Protocole facultatif se rapportant au Pacte international relatif aux droits civils et politiques, 19 décembre 1966, Organisation des Nations Unies, Recueil des Traités de l'ONU, vol. 999, p. 171, article 2.

Notes en fin de texte et références

* Préparé pour le compte du Commissariat à la protection de la vie privée (Canada) au nom de Mme Orla Lynskey (professeur associé, département de droit de la London School of Ecomomics (LSE) et de Judith Rauhofer (maître de conférences et directrice associée du Centre for Studies of Intellectual Property and Technology Law (SCRIPT), Université d'Édimbourg). Orla Lynskey est professeur associé de droit à la LSE et professeur invité au Collège d'Europe à Bruges. Elle mène des recherches et enseigne dans les domaines de la protection des données, des droits numériques

et de la réglementation des technologies. Ses recherches actuelles portent sur les défis juridiques et politiques liés à l'intégration des technologies du secteur privé dans l'infrastructure et le processus décisionnel du secteur public. Elle est rédactrice en chef de International Data Privacy Law et de Modern Law Review.

[1] *Résolution internationale sur la protection de la vie privée en tant que droit humain fondamental et condition préalable à l'exercice d'autres droits fondamentaux* (octobre 2019) - http://globalprivacyassembly.org/wp-content/uploads/2019/10/Resolution-on-privacy-as-a-fundamental-human-right-and-precondition-for-democracy-2019-FINAL-FR.pdf

[2] Voir, respectivement : Organisation de coopération et de développement économiques (OCDE), Lignes directrices sur la protection de la vie privée et les flux transfrontières de données à caractère personnel, 23 septembre 1980 (ci-après les Lignes directrices de l'OCDE sur la protection de la vie privée), telles que modernisées par la Recommandation du Conseil sur les Lignes directrices sur la protection de la vie privée et les flux transfrontières de données à caractère personnel (2013) [C(80)58/FINAL, telles que modifiées le 11 juillet 2013 par C(2013)79] (ci-après les Lignes directrices révisées de l'OCDE sur la protection de la vie privée); Conseil d'Europe, Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel, 28 janvier 1981, STE nº 108 (ci-après la Convention 108), telle que modernisée par le Protocole d'amendement de la Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel (STE nº 108), CM(2018)2-final, 18 mai 2018 (ci-après la Convention 108+); la Directive 95/46/EC du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JO L 281/31 23.11.1995 (ci-après la Directive de 1995), telle que modernisée par le Règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, abrogeant la Directive 95/46/EC, JO L 119, 4 mai 2016 (ci-après le RGPD).

[3] S. Landau. *Surveillance or security? The risks posed by new wiretapping technologies* (MIT Press, 2010), 10. [traduction] « La protection de la vie privée est un aspect fondamental d'une société humaine fonctionnelle, une nécessité évidente pour la liberté et la dignité humaines […] La protection de la vie privée comprend le droit de contrôler l'information qui vous concerne, le droit de vous associer avec qui bon vous semble, et d'une manière aussi privée que vous le souhaitez, de partager des confidences en toute confiance, le droit d'apprécier la solitude et l'intimité. Elle comprend également le droit à l'anonymité. »

[4] T. Oguru. « Electronic government and surveillance-oriented societies », in D. Lyon (dir.), *Theorizing Surveillance : the Panopticon and Beyond* (Routledge, 2006), 280. [traduction] « Les systèmes juridiques modernes sont arrivés à un point tournant important en ce qui concerne la réglementation du pouvoir politique; le droit cherche à réglementer le comportement humain, mais ne peut pas contrôler les ordinateurs […] La réglementation démocratique se fondant sur la primauté du droit a perdu son pouvoir de réglementation. »

[5] Haut-Commissaire des Nations Unies aux droits de l'homme. « Le droit à la vie privée à l'ère du numérique » (2018) - https://undocs.org/fr/A/HRC/39/29; voir aussi Rengel, Alexandra. « Privacy as an International Human Right and the Right to Obscurity in Cyberspace » (décembre 2014). *Groningen Journal of International Law*, vol. 2, nº 2, 2014. Accessible à https://ssrn.com/abstract=2599271.

[6] OCDE. Data-driven innovation for growth and well-being. Accessible à http://oe.cd/bigdata; voir aussi Martin Abrams. « The Origins of Personal Data and its Implications of Governance », Information Accountability Foundation (2016). Accessible à https://informationaccountability.org/publications/

[7] D. Acemoglu, et J. Robinson. *The Narrow Corridor: States, societies and the Fate of Liberty* (Penguin Random House, 2019), 492. « Les droits sont étroitement liés à notre notion de liberté, afin de protéger les gens de la peur, de la violence et de la domination. Même si la peur et la violence ont été les principaux facteurs de motivation […] La domination, c'est-à-dire l'incapacité des gens de faire des choix et de vivre leur vie en fonction de leurs propres valeurs, est également accablante. Les droits sont des façons fondamentales de permettre à la société d'intégrer à ses lois et normes la capacité de toutes les personnes à faire de tels choix. »

[8] W. Webster. « Public administration as surveillance », in Ball, Haggerty et Lyon (dir.), *Routledge Handbook of Surveillance Studies* (Routledge, 2012), 313. [traduction] « Dans un effort pour rendre le gouvernement et les services publics plus efficaces et rentables, d'énormes sommes ont été investies

dans l'infrastructure électronique, les bases de données et le gouvernement électronique […] Des sociétés se fondant sur des pratiques de surveillance permises par la technologie dépendent, en grande partie, de la plateforme et des appareils de surveillance créés par les administrations publiques... en faisant de la surveillance un aspect normal de la vie quotidienne. »

[9] Alan Westin. *Privacy and Freedom* (1967), 359.

[10] Canada. Ministère de la Justice. *L'ordinateur et la vie privée* : rapport du Groupe d'étude établi conjointement par le ministère des Communications et le ministère de la Justice (Ottawa, 1971), 10.

[11] Harold Innis. « Industrialism and cultural values », in *The Bias of Communication* (1951), 140.

[12] V. Mayer-Schönberger et K. Cukier. *Big Data: A Revolution That Will Transform How We Live, Work and Think* (John Murray, 2018), p. 83-84.

[13] Andy McStay. *Emotional AI* (Sage, 2018), 115.

[14] Voir le site Web d'EyeQ, accessible à https://eyeq.tech/retail/.

[15] S. Levin. « Facebook told advertisers it can identify teens feeling "insecure" and "worthless" », *The Guardian*, 1er mai 2017. Accessible à : https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens.

[16] D. Clifford. *The Legal Limits to the Monetisation of Online Emotions* (2019, thèse de doctorat, KU Leuven), 266-288. Accessible à : https://www.law.kuleuven.be/citip/en/research/phd-research/finalized/phd-damian-clifford.

[17] A. McStay. « Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy », janvier 2020, *Big Data & Society*, 1-12.

[18] Cohen souligne le tout, déclarant que [traduction] « dans le cadre des procédures gouvernementales et dans la presse populaire, les industries de traitement de l'information ont déployé des efforts pour opposer, de manière inextricable, l'innovation et les règlements en matière de protection. Cette stratégie a créé un processus discursif qui confère à l'innovation une signification particulière et subordonnée associée à la liberté économique et à l'absence de surveillance gouvernementale »; voir J. Cohen, *Between Truth and Power: The Legal Construction of Information Capitalism*, 2019, OUP, p. 90.

[19] Par exemple, on peut comparer les travaux de l'Ada Lovelace Foundation sur les données dans l'intérêt public - https://www.adalovelaceinstitute.org/our-work/library/, à des travaux semblables réalisés par la Royal Society sur l'utilisation de données dans l'intérêt public - https://royalsociety.org/blog/2020/07/using-data-for-the-public-good/, et à des travaux de l'OCDE sur l'amélioration de l'accès aux données et du partage de celles-ci - https://www.oecd.org/digital/ieconomy/enhanced-data-access.htm.

[20] Groupe de travail de la Société royale du Canada sur l'infoveillance (mars 2021) – https://rsc-src.ca/sites/default/files/Infoveillance_FR_0.pdf.

[21] J. Rauhofer. « Round and round the garden?: Big data, small government and the balance of power in the information age », in Erich Schweighofer, Franz Kummer, Walter Hoetzendorfer (dir.), *Transparenz* (OCG, 203), 2014, 606-617, p. 615.

[22] Pour obtenir une discussion sur l'utilisation d'algorithmes dans le système de justice pénale, voir : The Law Society of England and Wales. « Algorithms in the Criminal Justice System », juin 2019, p. 15-17.

[23] A. deNisco Rayome. « The US, China and the AI arms race: Cutting through the hype », CNet, 8 juillet 2020. Accessible à : https://www.cnet.com/news/the-us-china-and-the-ai-arms-race-cutting-through-the-hype/.

[24] S. Coughlan. « A-levels and GCSEs: Boris Johnson blames 'mutant algorithm' for exam fiasco », BBC, 26 août 2020. Accessible à : https://www.bbc.co.uk/news/education-53923279.

[25] W. Bedingfield. « Everything that went wrong with the botched A-Levels algorithm », Wired, 19 août 2020. Accessible à : https://www.wired.co.uk/article/alevel-exam-algorithm.

[26] Ibid.

[27] Evgeny Morozov. « The tech solutions for coronavirus take the surveillance state to the next level », *The Guardian* (15 avril 2020) - https://www.theguardian.com/commentisfree/2020/apr/15/tech-coronavirus-surveilance-state-digital-disrupt

[28] Voir, par exemple, Budd, J., Miller, B.S., Manning, E.M. et coll. Digital technologies in the public-health response to COVID-19. *Nat Med* 26, 1183–1192 (2020), https://doi.org/10.1038/s41591-020-1011-4, et, De', R., Pandey, N., et Pal, A. (2020). Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. *International journal of information management*, 55, 102171. https://doi.org/10.1016/j.ijinfomgt.2020.102171

[29] Zuboff. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books, 2019).
[30] Cicéron. *De Officiis (On Obligations),* traduction de P. G. Walsh (Oxford, 2008), livre I, art. 85, p. 30.
[31] F. D. Schoeman. *Privacy and social freedom* (1992), 116.
[32] Daniel Solove. *Understanding Privacy* (2008), p. 61-62.
[33] Laura K. Donohue. *The future of foreign intelligence: privacy and surveillance in a digital age* (Oxford, NY : 2016), p. 75-76.
[34] John H. Shattuck. *Rights of Privacy* (1977), p. 3-5
[35] Stanley A. Cohen. *Invasion of Privacy* (1983), p. 20-21, 34, 52
[36] James Madison. *Federalist Papers*, nº 51 (1788) - https://billofrightsinstitute.org/primary-sources/federalist-no-51; voir aussi Louis D. Brandeis et Samuel D. Warren. « The Right to Privacy ». *Harvard Law Review*, vol. 4, nº 5 (15 décembre 1890), p. 193-220. - http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C
[37] Georges Duby. « Introduction : Private Power, Public Power », in *A History of Private Life. II: Revelation of the Medieval World*, par Georges Duby (dir.) (Cambridge, MA : Belknap Press, 1988).
[38] Diane Shaw. « The Construction of the Private in Medieval London ». *Journal of Medieval and Early Modern Studies*, 26 (1996), p. 450.
[39] David Vincent. *Privacy: A Short History*. Wiley, 2016, p. 2.
[40] S.D. Warren et L.D. Brandeis. « The right to privacy ». 1890, 4, *Harvard Law Review*, p. 193-220. En fait, la phrase « droit d'être laissé tranquille » avait été prononcée par le juge Cooley plusieurs années avant cela. Voir T.M. Cooley, *A Treatise on the Law of Torts, Or the Wrongs Which Arise Independent of Contract,* (2e éd., Chicago, Callaghan & Company, 1880), p. 29.
[41] Ibid, p. 198.
[42] Alors que l'article 8 de la CEDH a eu de vastes répercussions sur la protection de la vie privée au sein des États membres du Conseil de l'Europe, le PIDCP de l'ONU a eu des répercussions moindres. Un comité des droits de la personne (CDP) regroupant des experts indépendants est chargé d'interpréter le PIDCP et d'assurer son respect. Le CDP oriente l'interprétation des dispositions du PIDCP en publiant des « observations générales » sur son interprétation. Il a déjà exercé ce pouvoir pour formuler une observation générale sur l'article 17 du PIDCP. Voir Observation générale nº 16, publiée le 23 mars 1988 (Doc. de l'ONU A/43/40, 181-183).
[43] Puisque ces rapports des États, lorsqu'ils sont présentés, n'évaluent pas obligatoirement avec exactitude le respect des droits prévus par le PIDCP par l'État en question, ils sont souvent accompagnés de rapports parallèles présentés par des organisations de la société civile. Le Comité discute de ces rapports avec les États parties, et adopte des observations et recommandations. Même s'il est bien vu que les États respectent ces recommandations, il n'existe aucun mécanisme pour les mettre en application. En plus de ce mécanisme de surveillance, lorsqu'un État a signé son premier protocole facultatif, le Comité peut recevoir des plaintes ou des pétitions d'individus.
[44] Ce chiffre se fonde sur une recherche réalisée dans la base de données de la jurisprudence du Haut-Commissariat des Nations Unies aux droits de l'homme. La base de données est accessible à : www.juris.ohchr.org (recherche valable en date du 10 septembre 2020).
[45] N. Sitaropoulos. « States are Bound to Consider the UN Human Rights Committee's Views in Good Faith ». (Blogue OxHRH, 11 mars 2015). Accessible à www.humanrights.dev3.oneltd.eu/states-are-bound-to-consider-the-un-human-rights-committees-views-in-good-faith/.
[46] HCDH des Nations Unies, « Rapports thématiques annuels du Rapporteur spécial sur le droit à la vie privée » – https://www.ohchr.org/FR/Issues/Privacy/SR/Pages/AnnualReports.aspx
[47] Voir aussi www.legal.un.org/ilc/.
[48] Dans le cas de l'Amérique latine, il faut évaluer les cas du Mexique et du Brésil. Au Mexique, la constitution reconnaît le droit à la vie privée depuis 1917. La loi sur la protection des données a été adoptée beaucoup plus tard, après les réformes constitutionnelles qui ont eu lieu pendant les années 1990 et 2000, qui reconnaissaient la protection des données de différentes manières. L'Amérique latine est unique, par exemple, lorsque vient le temps de codifier le concept d'« habeas data », la reconnaissance formelle du droit à l'accès aux renseignements propres à une personne et du droit de connaître ces renseignements. En revanche, dans la Constitution du Brésil, sous Égalité et non-discrimination, on peut lire que de [traduction] « nombreux cadres modernes de protection des données renferment un principe général de traitement personnel "juste", ce qui signifie qu'il n'est pas, entre autres, discriminatoire ». Le fait est que la non-discrimination dans la plupart des pays de la

région constitue une valeur en tant que telle, puisque les termes « équitable » ou « équité » ne se traduisent pas toujours fidèlement. La non-discrimination est une valeur au Brésil et aussi, par exemple, en Argentine, où elle est reconnue formellement dans la Constitution comme condition préalable de l'habeas data (art. 43).

[49] Voir les articles 6.A.II et III et l'article 16 de la Constitution du Mexique de 1917 (en sa version modifiée); l'article 13 de la Constitution de la Suisse de 1999 (en sa version modifiée); l'article 22 de la Constitution de la Belgique de 1831 (en sa version modifiée); l'article 17 de la Constitution de la République de Corée de 1987 (telle qu'amendée); les articles 2(11) et 3(3) de la Constitution des Philippines de 1987 (en sa version modifiée); l'article 30 de la Loi fondamentale de Hong Kong de 1982 (telle qu'amendée); l'article 6 de la Constitution du Portugal de 1976 (en sa version modifiée); l'article 15 de la Constitution de la Colombie de 1991 (telle qu'amendée); l'article 4(c) de la Constitution de Trinité-et-Tobago de 1976 (en sa version modifiée); l'article 1(5) et (12) de la Constitution du Gabon de 1991 (en sa version modifiée).

[50] L'article 7 de l'ordonnance constitutionnelle des Bermudes de 1968 (en sa version modifiée).

[51] Cela comprend les États de Brandebourg, de Mecklenburg-Poméranie, de Saxe, de Thuringe, de Saxe-Anhalt, de Schleswig-Holstein, d'Hesse, de Rhénanie-du-Nord–Westphalie, de Rhénanie-Palatinat et de la Sarre.

[52] BVerfGE 35, 202 – Lebach et BVerfGE 65, 1 - Loi sur le recensement.

[53] *Charte canadienne des droits et libertés*, articles 7 et 8, partie 1 de la *Loi constitutionnelle de 1982*, constituant l'annexe B de la *Loi de 1982 sur le Canada* (R.-U.), 1982, ch. 11.

[54] *Nihon-koku kenpō*, 3 mai 1947

[55] *Juge K.S.Puttaswamy (retraité) c. Union of India And Ors*., 2017, Writ Petition (Civil) nº 494 de 2012, (2017) 10 SCC 1.

[56] Charte de l'UE (nº **¡Error! Marcador no definido.** ci-dessus), article 51(1).

[57] Voir, en Autriche, BGBl. Nr. 59/1964, après avoir signé et ratifié la Convention en 1958, voir BGBl. Nr. 210/1958, et, au Royaume-Uni, la Loi sur les droits de l'homme de 1998 (LDH). Même si le Royaume-Uni est l'un des cofondateurs et l'un des premiers signataires de la CEDH, jusqu'à l'adoption de la Loi sur les droits de l'homme, les demandeurs devaient avoir épuisé tous les recours nationaux avant de pouvoir présenter un dossier en ce qui concerne les droits fondamentaux à la Cour européenne des droits de l'homme, à Strasbourg. Cependant, il faut souligner que même après l'entrée en vigueur de la Loi sur les droits de l'homme, en raison du principe constitutionnel de souveraineté parlementaire, les tribunaux ne peuvent pas invalider des lois du Parlement. Ils peuvent seulement fournir une « déclaration d'incompatibilité » de ces lois avec la CEDH. Il revient à l'organe de législation de modifier ou d'abroger la loi en question. Voir l'article 4 de la Loi sur les droits de l'homme.

[58] Datenschutzgesetz du 7 octobre 1970 (HDSG), GVBl. I, 625.

[59] Voir, par exemple, le Datalagen de la Suède en 1973 (Datalagen, 11 mai 1973), la première loi fédérale de l'Allemagne sur la protection des données de 1977 (Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung, Bundesdatenschutzgesetz (BDSG 1977), BGBl. I, 201), ainsi que d'autres lois nationales en France (Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés), au Danemark (Lov nr 294 af 8 juni 1978 om offentlige myndigheders register), en Norvège (Lov om personregistre mm av 9 juni 1978 nr 48) et en Autriche (Bundesgesetz über den Schutz personenbezogener Daten BGBl. 565/1978) en 1978, ainsi qu'au Luxembourg (Loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques) en 1979.

[60] Sur le plan historique, on pourrait donc faire valoir que les lois sur la protection des données relevaient, au départ, du droit primaire, plutôt que du droit constitutionnel. Les lois pertinentes peuvent être axées sur une loi privée ou une loi publique, en fonction du type d'utilisateurs de données qu'elles cherchent à réglementer. Cependant, il semble évident que le droit à la protection des renseignements personnels des individus n'était pas, en tant que tel, perçu au départ comme un droit fondamental autonome.

[61] Dans le jargon de l'UE, par « loi secondaire », on entend les lois non constitutionnelles de premier rang, alors que le terme « loi primaire » est réservé aux traités de l'UE.

[62] Clause d'introduction 11 de la Directive 95/46, « considérant que les principes de la protection des droits et des libertés des personnes, notamment du droit à la vie privée, contenus dans la présente directive précisent et amplifient ceux qui sont contenus dans la convention, du 28 janvier 1981, du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ».

[63] À l'époque, en raison de la nature variée de ces cadres nationaux, il était possible que des obstacles commerciaux étaient mis en place entre les États membres de l'UE, car les niveaux de protection fournis différaient. De plus, des États membres individuels étaient de plus en plus réticents à permettre les transferts transfrontaliers de renseignements personnels avec des pays qui offraient des niveaux de protection inférieurs.
[64] Article 1(1) de la Directive de 1995 (nº 2).
[65] Une version antérieure de la Charte a été préparée et solennellement proclamée le 7 décembre 2000, afin qu'elle soit éventuellement intégrée aux mécanismes constitutionnels contraignants de l'UE. Une version modifiée du texte original fait partie de la Constitution européenne proposée, qui devait remplacer les traités existants de l'UE par un seul texte. Cependant, même si la Constitution a été signée par tous les États membres à l'époque, le fait qu'elle n'ait pas été ratifiée par tous ces derniers a empêché son entrée en vigueur. Elle a finalement été abandonnée en 2004. Un droit à la protection des données est également établi à l'article 16 du traité sur le fonctionnement de l'Union européenne (TFUE), qui comprend l'obligation pour les organes législatifs de l'UE d'adopter des règles régissant le traitement des données personnelles par les institutions de l'UE et les États membres lorsqu'ils réalisent des activités touchées par les lois de l'UE.
[66] COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL : échange et protection de données à caractère personnel à l'ère de la mondialisation COM/2017/07 définitif – Point 3.3.1 - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN
[67] Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel. Rapport définitif présenté par Louis Joinet, rapporteur spécial, 21 juillet 1988 (E/CN.4/sous 2/1988/22).
[68] C. Kuner. « An International Legal Framework for Data Protection: Issues and Prospects ». (2009)25 *Computer Law and Security Review* 307, p. 309.
[69] Union européenne. Charte des droits fondamentaux de l'Union européenne [2012] JO C 326/02, article 8.
[70] Voir 27e Conférence internationale des Commissaires à la protection des renseignements personnels et de la vie privée, « Dans un monde globalisé, un droit universel à la protection des données personnelles et à la vie privée dans le respect des diversités », (2005), http://globalprivacyassembly.org/wp-content/uploads/2015/02/Montreal-Declaration-French.pdf. À cette fin, les commissaires ont également présenté les demandes suivantes : tous les gouvernements du monde devraient faire la promotion de l'adoption de mécanismes juridiques en matière de protection des données et de la vie privée en fonction des principes de base de la protection des données, en plus de les appliquer à leurs relations mutuelles; le Conseil de l'Europe devrait inviter, conformément à l'article 23 de la Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel, les États qui ne sont pas membres du Conseil de l'Europe disposant déjà de lois en matière de protection des données à devenir parties de cette Convention et de son protocole additionnel.
[71] Ibid., para. 12.
[72] Ibid., p. 3.
[73] CICPRPVP. Résolution de Madrid (novembre 2009) – http://privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf
[74] Voir, respectivement : Agencia Espanola de Proteccion de Datos, « Draft Joint Proposal for International Standards for the Protection of Privacy and Personal Data » (ébauche non publiée, janvier 2009; ébauches mises à jour datées du 24 février et du 24 avril 2009); Conférence internationale des commissaires à la protection des données et à la vie privée, « Resolution on anchoring data protection and the protection of privacy in international law » (2013), accessible à : www.globalprivacyassembly.org/wp-content/uploads/2015/02/International-law-resolution.pdf.
[75] Si l'on perçoit une telle coopération comme étant peu efficace, cela peut faire en sorte que certains sont réticents à intégrer la protection juridique internationale et à lui accorder plus d'importance que les normes nationales en matière de protection des données. Par exemple, les mécanismes existants de l'ONU sont peu reconnus sur la scène internationale.
[76] K.M. Yilma. « The United Nations data privacy system and its limits ». (2019) 33, *International Review of Law, Computers & Technology*, 224, p. 230.
[77] Voir P. de Hert et V. Papakonstantinou. « Three scenarios for international governance of data privacy: Towards an international data privacy organization, preferably a UN agency ». (2013)9 *Journal of Law and Policy* 271, p. 282.

[78] European Parliamentary report on the Commission Evaluation report on the implementation of the GDPR two years after its application (17 mars 2021) - https://www.europarl.europa.eu/doceo/document/B-9-2021-0211_EN.pdf; Access Now, *Two Years Under the EU GDPR: An Implementation Progress Report* (Mai 2020) - https://www.accessnow.org/cms/assets/uploads/2020/05/Two-Years-Under-GDPR.pdf; Nathan Eddy, « How EU Authorities See GDPR Effectiveness Two Years In », *e-Week* (17 juin 2020) - https://www.eweek.com/security/how-eu-authorities-see-gdpr-effectiveness-two-years-in/

[79] I/A Court H.R, affaire *Fontevecchia et D'Amico c. Argentine*, jugement du 29 novembre 2011 (bien-fondé, réparations et coûts, série C nº 238), para. 49

[80] Voir, par exemple, les affaires jointes C-92/09 et 93/09, *Volker et Markus Schecke et Eifert* UE : C : 2010 : 662, para. 89.

[81] Parmi les domaines de contestation constante, il y a la question de savoir s'il est possible de faire un rapprochement entre les avantages de l'innovation et la protection des droits fondamentaux, ainsi que la manière de le faire. On observait déjà des divisions à ce sujet pendant les années 1970, lorsque l'Assemblée générale de l'ONU a adopté la « Déclaration sur l'utilisation du progrès de la science et de la technique dans l'intérêt de la paix et au profit de l'humanité ». Les pays de l'ONU dans le Nord et l'Occident ont boycotté cette déclaration, et n'ont pas présenté de vote en ce qui concerne les résolutions subséquentes, car ces nations plus industrielles voulaient mettre l'accent sur les répercussions potentiellement négatives des développements technologiques sur les droits de la personne. Voir Yilma (nº **¡Error! Marcador no definido.**), p. 227 et 228.

[82] Kuner (nº **¡Error! Marcador no definido.**), p. 310.

[83] González Fuster G. 2014. « Privacy and the Protection of Personal Data Avant la Lettre », in *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Law, Governance and Technology Series, vol. 16. Springer, Cham. https://doi.org/10.1007/978-3-319-05023-2_2

[84] Cependant, comme Gonzalez-Fuster et Hijmans le soulignent, leur coexistence a soulevé de nombreuses questions, dont un très petit nombre ont « reçu une réponse d'une manière claire, uniforme ou consensuelle ». G. Gonzalez-Fuster et H. Hijmans. « The EU rights to privacy and personal data protection: 20 years in 10 questions », document de discussion, Brussels Privacy Hub. Accessible à : https://brusselsprivacyhub.eu/events/20190513.Working_Paper_González_Fuster_Hijmans.pdf.

[85] De manière générale, il cherche à permettre aux individus (« personnes visées ») de contrôler l'accès aux renseignements à leur sujet en faisant en sorte que le traitement des données personnelles fasse l'objet d'un consentement ou de lois qui autorisent ce traitement. Un droit à la protection des données accorde couramment aux personnes visées un certain nombre de droits reconnus par la loi, incluant notamment le droit d'accès à leurs données qui sont détenues par d'autres. Ce droit impose aux utilisateurs des données (les « contrôleurs ») un certain nombre d'obligations juridiques correspondantes.

[86] Par exemple, pour devenir membres de la Convention 108+, les États doivent avoir désigné une autorité indépendante chargée de la supervision (article 15(5), Convention 108+, nº 1 ci-dessus). Le paragraphe 8(2) de la Charte des droits fondamentaux de l'UE et l'article 16 du Traité sur l'Union européenne et du Traité sur le fonctionnement de l'Union européenne (version consolidée, journal officiel C 326, 26/10/2012 P. 0001-0390) indiquent tous les deux que le respect des règles en matière de protection des données doit faire l'objet d'un contrôle de la part d'une autorité indépendante.

[87] Par exemple, voir les règles et procédures détaillées par le service de recherche du Congrès américain dans son rapport intitulé *Data Protection Law : An Overview* (mars 2019). Accessible à https://fas.org/sgp/crs/misc/R45631.pdf.

[88] W. Veil. « The GDPR: The Emperor's New Clothes - On the Structural Shortcomings of Both the Old and the New Data Protection Law ». (2018), p. 22. Accessible sur le site du SSRN : https://ssrn.com/abstract=3305056

[89] O. Lynskey. *The Foundations of EU Data Protection Law* (OUP, 2015), p. 91-105.

[90] P. de Hert et S. Gutwirth. « Privacy, data protection and law enforcement. Opacity of the individual and transparency of power », in Claes et coll. (dir.), *Privacy and the criminal law* (Intersentia, 2006) 61, p. 66-67.

[91] D. Solove. *The Digital Person: Technology and Privacy in the Information Age* (NYU Press, 2004), p. 8.

[92] G. Gonzalez-Fuster. *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer, 2004), p. 257.

[93] O. Lynskey. « Deconstructing Data Protection: The "Added-Value" of a Right to Data Protection in the EU Legal Order » (2014) 63 *International and Comparative Law Quarterly* 569, p. 584-585.
[94] Mark Chinen. « Complexity Theory and the Horizontal and Vertical Dimensions of State Responsibility ». *European Journal of International Law*, volume 25, numéro 3, août 2014, p. 703-732, https://doi.org/10.1093/ejil/chu048
[95] Corrin, Jennifer. « From Horizontal and Vertical to Lateral: Extending the Effect of Human Rights in Post-Colonial Legal Systems of the South Pacific ». *The International and Comparative Law Quarterly* 58, nº 1 (2009) : p. 31-71. Consulté le 30 juillet 2021. http://www.jstor.org/stable/20488273.
[96] P. De Hert et S. Gutwirth. « Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action », in S. Gutwirth et coll. (dir.), Reinventing Data Protection? (Springer 2009) 5, p. 8.
[97] Lynskey (nº **¡Error! Marcador no definido.**), p. 586-587.
[98] AF Westin. *Privacy and Freedom* (1967, Atheneum), p. 324-325.
[99] Gavison, Ruth E. Privacy and the Limits of Law, 16 mai 2012. *The Yale Law Journal,* vol. 89, nº 3 (janvier 1980), pp. 421-471. Accessible sur le site du SSRN : https://ssrn.com/abstract=2060957, ou Zuboff, Shoshana. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization (4 avril 2015). *Journal of Information Technology* (2015) 30, 75–89. Doi:10.1057/jit.2015.5. Accessible sur le site du SSRN : https://ssrn.com/abstract=2594754
[100] Pour une explication plus approfondie de cette distinction, voir Gonzalez-Fuster et Hijmans (nº **¡Error! Marcador no definido.**) p. 6.
[101] R. Post. « Data Privacy and Dignitary Privacy: Google Spain, the Right to be Forgotten, and the Construction of the Public Sphere ». (2018) 67, *Duke Law Journal*, 980, 1011.
[102] C.J. Hoofnagle, B. van der Sloot et F.Z. Borgesius. « The European Union general data protection regulation: what it is and what it means » (2019) 28 *Information & Communications Technology Law* 65.
[103] L. Dalla Corte. « A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection », in D. Hallinan et al. (éd.), *Data Protection and Privacy: Data Protection and Democracy* (Hart, 2020) p. 27; voir aussi Veil (nº **¡Error! Marcador no definido.**) p. 22.
[104] H. Hijmans. *The European Union as Guardian of Internet Privacy* (Springer, 2016), parag. 2.13.
[105] N. Andrade. « Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights », p. 7. Accessible à : www.hal.inria.fr/hal-01559453.
[106] A. Rouvroy et Y. Poullet. « The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy », in S. Gutwirth et al. (éd.), *Reinventing Data Protection?* (Springer 2009), p. 45.
[107] Andrade suggère, par exemple, que [traduction] « ce n'est qu'après l'évaluation des intérêts et droits substantiels en question et l'établissement d'un équilibre entre ceux-ci que les droits procéduraux entrent en jeu, établissant les conditions et procédures juridiques au moyen desquelles ces droits substantiels seront mis efficacement en application ». Andrade (nº **¡Error! Marcador no definido.**) 6.
[108] En ce qui concerne la Loi constitutionnelle américaine, on continue de débattre de la question de savoir si le cours normal de la loi est un droit substantiel ou procédural. Malgré tout, son statut de droit constitutionnel n'a jamais été remis en question. On pourrait affirmer la même chose au sujet du droit à un procès juste, droit reconnu par de multiples mécanismes juridiques internationaux. Plus récemment, des droits environnementaux procéduraux ont été intégrés à des documents constitutionnels nationaux et à des accords juridiques internationaux.
[109] Haut-Commissariat des Nations Unies aux droits de l'Homme. *General Comment on Article 9 of UN CRPD (Accessibility*) - https://www.ohchr.org/EN/HRBodies/CRPD/Pages/GC.aspx
[110] Article 1, Charte de l'UE (nº **¡Error! Marcador no definido.**). Même si la CEDH ne prévoit pas formellement un droit à la dignité humaine, son Protocole nº 13 à la Convention de sauvegarde des droits de l'homme et des libertés fondamentales relative à l'abolition de la peine de mort en toutes circonstances renvoie à la nécessité de reconnaître pleinement « la dignité inhérente à tous les êtres humains ».
[111] I. Kant. *Fondements de la métaphysique des mœurs,* traduction de Victor Delbos, Éditions Les Échos du Maquis, 2013, p. 88 (mise en évidence omise).
[112] D. Lyon. *The Electronic Eye: The Rise of Surveillance Society* (University of Minnesota Press, 1994), p. 109.
[113] D. Keats Citron et F. Pasquale. « The Scored Society: Due Process for Automated Predictions » (2014) 89, *Washington Law Review*, 1, 3.

[114] Colin J. Bennett. « In Defence of Privacy: the concept and the regime », in *Surveillance and Society* 8(4) 2011, p. 485-496 - https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/4184/privacy_debate
[115] Frederik J. Zuiderveen Borgesius. *Improving Privacy Protection in the Area of Behavioural Targeting*, Kluwer Law International, 2015, p. 43.
[116] Justin Sherman. « Data Brokers Are A Threat To Democracy ». *Wired*, avril 2021 - https://www.wired.com/story/opinion-data-brokers-are-a-threat-to-democracy/
[117] Lyon (nº 112), p. 13.
[118] K. Crawford et J. Schultz. « Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms ». (2014) 55, *Boston College Law Review*, 93, p. 111.
[119] Lyon (nº 112), p. 70-71. Voir aussi A. Spina, « Risk Regulation of Big Data: Has the Time Arrived for a Paradigm Shift in EU Data Protection Law? ». (2014) 2 *European Journal of Risk Regulation*, 248, p. 251.
[120] J. Raz. *The Morality of Freedom* (Oxford University Press, 1986), p. 369.
[121] « Invictus », WE Henley in « A Book of Verses » (D. Nutt, 1888), p. 56-57.
[122] Acquisti, Alessandro, Curtis Taylor, et Liad Wagman. 2016. « The Economics of Privacy ». *Journal of Economic Literature*, 54 (2) : 442-92 - https://www.aeaweb.org/articles?id=10.1257/jel.54.2.442
[123] Par exemple, voir Fred H. Cate, « The Failure of Fair Information Practice Principles », in *Consumer Protection in the Age of the Information Economy* (2006) – https://www.ftc.gov/system/files/documents/public_comments/2018/12/ftc-2018-0098-d-0036-163372.pdf
[124] TI Emerson, *The system of freedom of expression* (Random House Trade, 1970), p. 549.
[125] Regan, Priscilla M. Legislating Privacy: Technology, Social Values and Public Policy. Chapel Hill, NC: University of North Carolina Press, 1995;
[126] Sur la marchandisation, voir : C Prins, « When personal data, behavior and virtual identities become a commodity: Would a property rights approach matter » (2006)3 SCRIPTed 270.
[127] Greenleaf, Graham, Global Tables of Data Privacy Laws and Bills (7e éd., janvier 2021) (11 février 2021). (2021) 169 *Privacy Laws & Business International Report.* 6-19, accessible à l'adresse suivante : https://ssrn.com/abstract=3836261 ou http://dx.doi.org/10.2139/ssrn.3836261
[128] Graham Greenleaf, A*sian Data Privacy Laws: Trade and Human Rights Perspectives* (Oxford University Press, 2014) and *Regulation of Cross-Border Transfers of Personal Data in Asia* (Asian Business Law Institute, 2018) - https://abli.asia/PUBLICATIONS/Regulation_of_Cross-border_Transfers_of_Personal_Data_in_Asia
[129] On peut citer l'exemple de Singapour et de sa politique sur les droits de la personne qui s'appuie sur des objectifs d'État et de développement national primordiaux priorisant la croissance économique et l'ordre social. La portée et l'application des droits de la personne sont encadrées par les impératifs du développement économique et la référence culturelle au communautarisme néo-confucéen. Voir le professeur Thio Li-Ann, « Pragmatism and realism do not mean abdication: a critical and empirical inquiry into Singapore's engagement with international human rights law » in *Singapore Year Book of International Law* (2004) 8, p. 41-91 - http://www.asianlii.org/sg/journals/SGYrBkIntLaw/2004/4.pdf.
[130] Par exemple, certaines des plus anciennes lois sur la protection des données au monde proviennent de pays d'Asie-Pacifique comme Hong Kong, la Nouvelle-Zélande, l'Australie, la Corée du Sud et le Japon. Bien que ces lois soient maintenant solides et efficaces, elles sont fondées sur des obligations et des droits organisationnels pour les personnes concernées plutôt que sur la protection des droits de la personne.
[131] La Chine, l'UE et les États-Unis ont adhéré à l'initiative Osaka Track, alors que l'Inde, l'Indonésie et l'Afrique du Sud ont refusé, ce qui creuse un fossé évident dans l'avenir des négociations sur le commerce électronique et la gouvernance des données à l'OMC.
[132] La vision de politique étrangère de l'Inde en matière de normes de protection des données est étroitement liée aux concepts de « souveraineté des données » ou, plus important encore, de « colonialisme des données » (qui s'apparente à la notion de capitalisme de surveillance de Zuboff). Voir Arindrait Basu, « Sovereignty in a "datafied" world: A framework for Indian diplomacy » at *Observer Research Foundation* (2 mai 2021) - https://www.orfonline.org/expert-speak/sovereignty-datafied-world-framework-indian-diplomacy
[133] Voir par exemple, « Asia's Family Values Give Way to Data Privacy Concerns » https://www.voanews.com/silicon-valley-technology/asias-family-values-give-way-data-privacy-

concerns, et IAPP, « Why China's cultural attitudes toward privacy may be in flux » - https://iapp.org/news/a/why-chinas-cultural-attitudes-toward-privacy-may-be-in-flux/
[134] K. Kitiyadisai, « Privacy rights and protection: foreign values in the modern Thai context » (2005)7 *Ethics and Information Technology* 17, p. 19.
[135] H.N. Olinger, J.J. Britz, et M.S. Olivier « Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa » (2007)39 *The International Information & Library Review* 31, p. 34.
[136] Ibid., p. 35.
[137] Ibid.
[138] Cet argument est avancé, par exemple, par Shoshana Zuboff. Voir S. Zuboff. *L'âge du capitalisme de surveillance : le combat pour un avenir humain face aux nouvelles frontières du pouvoir*, Éditions Zulma, 2020.
[139] *Histoire de la vie privée : De l'Empire romain à l'an mil*, vol. 1, éd. Paul Veyne, Seuil, 1985, p. 415
[140] Evgeny Morozov, *To Save Everything, Click Here: the folly of technological solutionism* (2013), 346; voir aussi Ursula Franklin, « Liberty, technology and hope » in *The Ursula Franklin Reader* (2006), 172
[141] John Stuart Mill, *De la liberté*, traduit de l'anglais par Laurence Lengle, Paris, Éditions Gallimard, 1990, p. 7-8.
[142] De plus, dans un contexte informatif, il a bien souvent été difficile de trouver un réel préjudice aux intérêts d'une personne, sans parler des intérêts des autres ou de la communauté. Par contre, de nouvelles méthodes d'utilisation (abusive ou non) des données ont montré que de tels intérêts collectifs ne devraient pas être ignorés lorsque l'on envisage la nécessité et la portée de ces droits.
[143] Voir la remarque **¡Error! Marcador no definido.**.
[144] Dans le passé, des annonceurs en ligne ont indiqué que le simple suivi des internautes par des témoins ne devrait être assujetti à aucune forme de réglementation, car, selon eux, « aucun préjudice n'est causé » et que les règles de protection de la vie privée et des données ne devraient être appliquées que si les données sur le comportement des utilisateurs sont exploitées et s'ils créent des profils de comportement des utilisateurs.
[145] En 1962, l'Assemblée générale des Nations unies a reconnu le « droit des peuples et des nations à la souveraineté permanente sur leurs richesses et ressources naturelles ». Voilà une définition claire non seulement des intérêts du groupe, mais aussi de son droit d'avoir son mot à dire sur les ressources jugées essentielles pour les intérêts collectifs du groupe. Voir Malcolm Shaw, *International Law, Fifth Edition* (2003, Cambridge University Press).
[146] Cette approche est particulièrement flagrante dans le secteur public où divers joueurs jugent nécessaire d'avoir accès aux données détenues par d'autres services ou par des entreprises afin de défendre les intérêts légitimes du public comme la sécurité, la santé publique ou l'utilisation responsable des fonds publics.
[147] P Ohm, « Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization » (2010)57 *UCLA Law Review* 1701, p. 2010
[148] J. Rauhofer (n **¡Error! Marcador no definido.**), pp. 606-617.
[149] J. Cohen (n 18), p. 72.
[150] M. Adrejevic, « iSpy: Surveillance and Power in the Interactive Era », (University Press of Kansas, 2007), pp. 2-4 et 104-11.
[151] Alinéa 5(1)(c) RGPD.
[152] Zuboff, *L'âge du capitalisme de surveillance : le combat pour un avenir humain face aux nouvelles frontières du pouvoir*, Éditions Zulma, 2020, p. 7.
[153] Pourtant, certains craignent que le profilage et le ciblage ultérieur des personnes n'entraînent une discrimination par le prix et les pratiques de commercialisation déloyales à l'égard de certains groupes de consommateurs. Pour un examen plus récent de ces questions, voir N. Newman, « The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google » (2013); accessible au SSRN : http://ssrn.com/abstract=2310146, consulté le 20 octobre 2020.
[154] Pour un examen détaillé de ce phénomène, voir E. Pariser, *The Filter Bubble: What The Internet Is Hiding From You* (Penguin Books, 2011).
[155] Il ressort aussi de façon assez importante que cette utilisation particulière des données personnelles (profilage et ciblage de personnes) a au moins été très efficace pour transmettre certains messages politiques à un public plus large, en exploitant le mécontentement et en connectant les personnes aux vues similaires comme jamais auparavant. Bien entendu, comme toutes les technologies, ces outils peuvent être utilisés à bon ou mauvais escient (c'est une question

d'opinion), mais la diffusion des techniques de surveillance comportementale peut néanmoins, comme l'affirme Cohen, avoir « produit des moyens puissants pour la volatilité, la polarisation et l'intransigeance publiques » Cohen (n 18), p. 86.
[156] L'utilisation de l'énergie nucléaire, le préjudice environnemental ou certains types de recherche sont souvent cités comme éléments de comparaison.
[157] J. Cohen (n 18), p. 90
[158] P.M. Regan, *Legislating Privacy: Technology, Social Values and Public Policy* (University of North Carolina Press, 1995), p. 230.
[159] Ibid, p. 233.
[160] S. Simitis, « Reviewing Privacy in an Information Society » (1987)135 *University of Pennsylvania Law Review* 709.
[161] Avec une rare clairvoyance, Simitis a aussi suggéré que de savoir qui peut accéder aux données personnelles et ce qu'il peut en faire ne devrait plus être une préoccupation essentiellement individuelle (par exemple, celle des célébrités qui souhaitent cacher leurs activités à un public curieux), mais que la discussion doit tenir compte des intérêts publics ou collectifs. Selon lui, cette constatation s'applique notamment au traitement de données omniprésent qui normalise la surveillance du public par les personnes au pouvoir et les aide à déterminer et à appliquer des normes juridiques et sociales.
[162] Ibid, p. 734. Voir aussi S. Simitis, « Die informationelle Selbstbestimmung—Grundbedingung einer verfassungskonformen Informationsordnung » (1984) *Neue Juristische Wochenschrift*, 394–405, p. 399.
[163] S. Simitis, n 160.
[164] Bien que la Cour ait établi le droit à l'autodétermination informationnelle dans le but d'accorder à toute personne un contrôle (restreint) sur ses données personnelles, (l'une) des raisons sous-jacentes à l'octroi de cette protection était de leur donner les moyens d'exercer ces droits au profit de leurs communautés.
[165] Voir n **¡Error! Marcador no definido.**.
[166] Observation générale (n **¡Error! Marcador no definido.**) para. 3 et 7.
[167] Les affirmations selon lesquelles la protection des données et la protection de la vie privée empêchent la réalisation d'autres droits et intérêts omettent souvent d'appliquer ce moyen de conciliation de manière appropriée, voire de comprendre qu'une telle conciliation est possible.
[168] UN Office of the High Commissioner for Human Rights, *Article 19: Freedom of Opinion and Expression* – https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23944&LangID=E
[169] Voir, par exemple, le paragraphe 8(2) de la CEDH. Partant du principe que la sécurité nationale vise à protéger le droit à la vie, il est souvent difficile de faire valoir qu'un équilibre doit quand même être trouvé entre ces deux intérêts. Pourtant, la sécurité est aussi une question de perspective et de modèle de menace utilisé pour justifier les atteintes à la vie privée. Les partisans de la restriction des droits fondamentaux dans l'intérêt de la sécurité invoquent généralement un modèle de menace tourné vers l'extérieur, à savoir la possibilité d'une attaque en situation de terrorisme ou de crime organisé. Les mesures de sécurité préconisées dans cette situation sont généralement présentées comme un moyen pour l'État de protéger les personnes dont les droits à la vie privée ou à la protection des données peuvent être enfreints. L'équilibre à établir est ainsi représenté comme un jeu de gagnant-perdant où une augmentation de la sécurité (assurée par l'État) exigera une ingérence dans la vie privée de la personne (perpétrée par l'État). En revanche, il existe en parallèle d'autres modèles de menace qui méritent d'être pris en compte quand l'équilibre entre vie privée et sécurité est trouvé. Un de ces modèles de menace est orienté vers l'intérieur, à savoir la menace à laquelle les personnes, seules et collectivement, sont exposées en présence d'un modèle de gouvernance autoritaire ou totalitaire. Les instruments de défense des droits de la personne ont en grande partie été créés comme des droits de défense négatifs destinés à protéger la personne contre un État autoritaire. Dans ce contexte, la sécurité pourrait donc être définie comme la protection contre ces mêmes institutions qui veulent justifier la nécessité d'interférer avec les droits et libertés de la personne sans tenir compte des protections offertes par ces instruments. À cet égard, les personnes se prévalent du droit à la vie privée et à la protection des données justement pour contrer la menace posée par l'État non seulement à leur sécurité personnelle, mais aussi aux institutions démocratiques dont le mandat est de protéger leurs droits et libertés. La question de savoir si la sécurité exige l'atteinte ou la protection des renseignements personnels dépend donc de comment la menace est formulée.

[170] Voir *Klass c. Allemagne* et *Amann c. Suisse* (n **¡Error! Marcador no definido.**).
[171] Voir *Arrêt de la cour (grande chambre) dans l'affaire C-746/18 Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques)* (n 45).
[172] Nations Unies, *Rapport du Rapporteur spécial sur les droits à la liberté de réunion pacifique et à la liberté d'association au Conseil des droits de l'homme* (mai 2019) - https://undocs.org/fr/A/HRC/41/41
[173] C.J. Benett et C.D. Raab, *The Governance of Privacy* (2e éd., MIT Press, 2006) p. 23.
[174] Dans d'autres domaines, il faut y entendre que la commodité et l'efficacité que les entités publiques et privées tirent de la création de grandes bases de données (par exemple, les dossiers médicaux nationaux centralisés) ou de méthodes de surveillance continue (comme la STCF, les technologies de reconnaissance faciale ou le suivi comportemental en ligne) doivent avoir comme pendant les risques d'abus. Des dispositifs de sécurité techniques et réglementaires efficaces peuvent empêcher « l'état des bases de données » de devenir l'équivalent virtuel du « bâtiment panoptique » de Jeremy Bentham, le célèbre modèle de prison où les détenus pouvaient être surveillés à partir d'un point central sans qu'ils sachent quand, ou même si'ils étaient observés. En effet, le « regard inégal » qui caractérise ce type de surveillance risque de provoquer l'assimilation d'un état d'esprit disciplinaire chez les personnes observées. Bien que, d'une part, les personnes continuellement observées sont moins susceptibles d'enfreindre les règles ou les lois, d'autre part, il est possible de les dissuader d'exercer leurs droits et libertés individuels ou de participer en général au processus démocratique.
[175] E. Bloustein, « Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser » (1964) 39 *New York University Law Review* 1000.
[176] D. Lyon, *Surveillance after September 11* (Polity Press, 2003), p. 27.
[177] C'est la prémisse du film « Rapport minoritaire », dans lequel les forces de l'ordre ont trouvé un moyen de prédire un crime et sont en mesure de l'empêcher. Malheureusement, la méthode de prédiction n'a pas été infaillible. Les membres des catégories « suspectes » (par exemple, les membres des communautés musulmanes) peuvent assimiler ces soupçons; ils se sentent ainsi observés et évitent toutes activités et associations qui pourraient être mal interprétées. On ouvre ainsi la porte à une diminution de la participation politique de certains groupes minoritaires, ce qui pourrait endommager le tissu politique d'une société démocratique. On pourrait aussi inciter les membres de ce groupe à se tourner vers d'autres formes de protestation et de résistance et, en bout de piste, à les marginaliser de la société et de ses valeurs.
[178] Lyon (n 176) p. 142
[179] Ibid.
[180] P.M. Regan (n 158), p. 227
[181] Benett et Raab (n 173).
[182] Rapporteur spécial de l'ONU sur le droit à la vie privée, Évaluation préliminaire des aspects de la pandémie de maladie à coronavirus (COVID-19) liés à la vie privée (juillet 2020) - https://undocs.org/fr/A/75/147
[183] Un autre exemple pourrait être que la Cour suprême israélienne a interdit aux services de sécurité israéliens de continuer à accéder aux données mobiles des citoyens sans autorisation législative précise. (Utilisation non consensuelle). Voir Reuters, « Israel's top court says government must legislate COVID-19 phone-tracking » (26 avril 2020) - https://www.reuters.com/article/us-health-coronavirus-israel-monitoring-idUSKCN2280RN
[184] B. Petkova, « Privacy as Europe's First Amendment » (2019)25 *European Law Journal* 140, p. 152.
[185] D. Kaye, « Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression », Human Rights Council: Twenty-ninth session, agenda item 3, 22 mai 2015, p. 15.
[186] N.M. Richards, *The Dangers of Surveillance*, (2013)126 *Harvard Law Review* 1934, pp. 1945-1952.
[187] Ibid, p. 1935.
[188] Ibid, p. 1948.
[189] *Open Door et Dublin Well Woman c. Irlande*, requête n° 14235/88 [1992] CEDH 68, 29 octobre 1992.
[190] Ibid, para. 81.
[191] ONU, Comité des droits de l'enfant, *Observation générale no 25 (2021) sur les droits de l'enfant en relation avec l'environnement numérique* (mars 2021) -

https://digitallibrary.un.org/record/3906061?ln=en; voir aussi Women's Legal Education and Action Fund (LEAF), De-platforming misogyny (avril 2021) - https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf

[192] Marie-Claude Landry (présidente de la Commission canadienne des droits de la personne) : « Le développement de nouvelles technologies fait en sorte qu'il est plus important que jamais d'être protégés contre la discrimination génétique [...] Nous continuerons d'encourager les gouvernements provinciaux et territoriaux à apporter des améliorations similaires à leur propre législation en matières des droits de la personne. La technologie et la vie privée sont essentielles pour la prochaine génération des droits de la personne. Toutes les personnes au Canada devraient pouvoir prendre avantage de la technologie sans aucune crainte. » (juillet 2020) - https://www.chrc-ccdp.gc.ca/fr/ressources/decision-de-la-cour-supreme-du-canada-victoire-pour-la-protection-des-droits-de-la

[193] ONU, Comité des droits de l'enfant, *Observation générale nº 25 (2021) sur les droits de l'enfant en relation avec l'environnement numérique* (mars 2021) - https://digitallibrary.un.org/record/3906061?ln=en; voir aussi Women's Legal Education and Action Fund (LEAF), De-platforming misogyny (avril 2021) - https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf

[194] UN Committee issues recommendations to protect children's rights in digital environment https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=26944&LangID=E

[195] https://www.unicef.org/globalinsight/featured-projects/ai-children

[196] ONU, Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression. https://undocs.org/pdf?symbol=fr/A/73/348. - *AI and Human Rights 2018 AI-and-FOE-GA.pdf*. https://freedex.org/wp-content/blogs.dir/2015/files/2018/10/AI-and-FOE-GA.pdf.

[197] *The OECD Artificial Intelligence Policy Observatory*. https://www.oecd.ai/; Livre blanc sur l'intelligence artificielle – Une approche européenne axée sur l'excellence et la confiance| Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/consultations/white-paper-artificial-intelligence-european-approach-excellence-and-trust. *Kung - L'ère de l'IA : rapport sur les stratégies nationales et régionales en matière d'IA.* https://cifar.ca/wp-content/uploads/2020/11/l-ere-de-l-ia-deuxieme-edition-f.pdf. « Conseil de l'Europe et intelligence artificielle », *Intelligence artificielle*, https://www.coe.int/fr/web/artificial-intelligence/home
Décoder l'intelligence artificielle : 10 mesures pour protéger les droits de l'homme. https://rm.coe.int/decoder-l-intelligence-artificielle-10-mesures-pour-proteger-les-droit/168094b6e2. .

[198] *Artificial Intelligence: Governance and Leadership Whitepaper (2019) | Australian Human Rights Commission*. https://humanrights.gov.au/our-work/rights-and-freedoms/publications/artificial-intelligence-governance-and-leadership.

[199] *Human Rights in the Age of Artificial Intelligence - AI-and-Human-Rights.Pdf*. https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf.

[200] Policy Guidance on AI for Children: *Draft for consultation | Recommendations for building AI policies and systems that uphold child rights* https://www.unicef.org/globalinsight/reports/policy-guidance-ai-children

[201] Krishnamurthy, Vivek. « It's Not Enough for AI to Be 'Ethical'; It Must Also Be 'Rights Respecting », *Medium*, 10 octobre 2018, https://medium.com/berkman-klein-center/its-not-enough-for-ai-to-be-ethical-it-must-also-be-rights-respecting-b87f7e215b97 ; Raso, Filippo A., et coll. *Artificial Intelligence & Human Rights: Opportunities & Risks*. SSRN Scholarly Paper, ID 3259344, Social Science Research Network, 25 septembre 2018. *papers.ssrn.com*, doi:10.2139/ssrn.3259344.

[202] Comme le Groupe de travail intergouvernemental à composition non limitée sur les sociétés transnationales et autres entreprises et les droits de l'homme, dont le mandat est d'élaborer un instrument international juridiquement contraignant pour réglementer, dans le cadre du droit international des droits de l'homme, les activités des sociétés transnationales et autres entreprises. https://www.ohchr.org/FR/hrbodies/hrc/wgtranscorp/pages/igwgontnc.aspx; https://www.ohchr.org/Documents/HRBodies/HRCouncil/WGTransCorp/OEIGWG_RevisedDraft_LBI.pdf

[203] Et « Intelligence artificielle, la PDA et le système de justice », LCO-CDO, https://www.lco-cdo.org/en/our-current-projects/ai-adm-and-the-justice-system/.

[204] Revised draft U.N. treaty on business and human rights: a few steps forward, a few unanswered questions https://www.accessnow.org/revised-draft-u-n-treaty-on-business-and-human-rights-a-few-steps-forward-a-few-unanswered-questions/

[205] Société royale du Canada, *INFOVEILLANCE*. https://rsc-src.ca/fr/infoveillance-fr.

[206] Commissariat à la protection de la vie privée du Canada, *Communiqué : Le commissaire encouragé par les propositions de réforme de la loi du secteur public*, le 24 mars 2021, https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2021/nr-c_210324/.
[207] *Equinet Report : Regulating for an Equal AI: A New Role for Equality Bodies.* *https://equineteurope.org/2020/equinet-report-regulating-for-an-equal-ai-a-new-role-for-equality-bodies/*
[208] O. De Schutter et J. Ringelheim, « Ethnic Profiling: A Rising Challenge for European Human Rights Law » (2008) 71 *Modern Law Review* 358.
[209] M. Veale et R. Binns, « Fairer Machine Learning in the Real World: Mitigating Discrimination without Collecting Sensitive Data » (2017)4 *Big Data & Society*. Accessible à l'adresse : https://journals.sagepub.com/doi/epub/10.1177/2053951717743530.
[210] Résolution (74) 29 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur public; adoptée par le Comité des Ministres le 20 septembre 1974, lors de la 236e réunion des Délégués des Ministres. Annexe, para. 3.
[211] G. Malgieri, « The concept of fairness in the GDPR: a linguistic and contextual interpretation », FAT* « 20: Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (ACM, 2020). pp. 154-166.
[212] Dispõe sobre a proteção de dados pessoais e altera a Lei no 12.965, de 23 de abril de 2014 (Marco Civil da Internet), Article IX.
[213] CNIL, « Comment permettre à l'Homme de garder la main? Les enjeux éthiques des algorithmes et de l'intelligence artificielle » (2017), p. 49. Accessible à l'adresse : https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf.
[214] Selon Greenleaf (2016), à la fin de chaque décennie, le nombre de lois est passé de 10 (années 1970) à 20 (années 1980), à 40 (années 1990), à 80 (années 2000), et maintenant à 111 (aux deux tiers des années 2010). Il mentionne que « l'indicateur le plus frappant de la mondialisation des lois protégeant les renseignements personnels est que, depuis 2015, la plupart de ces lois (57/111) proviennent de pays non européens ». G. Greenleaf, « Balancing globalisation's benefits and commitments: accession to data protection convention 108 by countries outside Europe » [2016] UNSWLRS 52, p. 1.
[215] Avis n° 934/2018, Commission européenne pour la démocratie par le droit (Commission de Venise), Luxembourg – Proposition de révision portant instauration d'une nouvelle constitution, Strasbourg, le 27 février 2019 (Rapport de la Luxembourg, CDL-REF (2019)006); voir aussi, TA Larsen, C Boulanger et A Vandendriessche, « Luxembourg » in *The New EU Data Protection Regime: Setting Global Standards for the Rights to Personal Data Protection* (The Hague, 2020), 411 et 412.
[216] *Puttaswamy* (n **¡Error! Marcador no definido.** ci-dessus), para 169.
[217] La loi philippine sur la confidentialité des données de 2012 (loi n° 10173) s'inspire en partie de la proposition législative de la Commission européenne pour le RGPD. Elle contient notamment un droit à la portabilité des données (article 18) dont le libellé est similaire au droit qui figure désormais à l'article 20 du RGPD et qui est par ailleurs propre au RGPD.
[218] Convention 108+ (n 2), para. 37(1) et (2).
[219] Ibid, para. 4(3).
[220] Voir la présentation de la professeure Cécile De Terwangne, « Convention 108+ evaluation and follow-up mechanisms », 1er juillet 2020. Accessible à l'adresse : https://www.coe.int/en/web/data-protection/follow-up-and-evaluation-mechanism.
[221] Les signataires non européens de la Convention 108 sont l'Argentine, le Cap Vert, Maurice, le Mexique, le Maroc, le Sénégal, la Tunisie et l'Uruguay (https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=TAAIBf9O). Parmi eux, l'Argentine, Maurice, la Tunisie et l'Uruguay ont signé la Convention 108+ et Maurice l'a aussi ratifiée (https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/223/signatures).
[222] Les États non européens qui adhèrent jusqu'à l'entrée en vigueur du protocole d'amendement devront présenter des instruments d'adhésion pour la Convention 108 et le protocole d'amendement. Une liste des observateurs (mise à jour pour la dernière fois en mars 2020) est disponible à l'adresse suivante : https://rm.coe.int/list-of-observers-nov-2018-fr/1680938538.
[223] Colin J. Bennett, « The Council of Europe's Modernized Convention on Personal Data Protection: Why Canada Should Consider Accession » CIGI Paper No. 246 (30 novembre 2020) - https://www.cigionline.org/publications/council-europes-modernized-convention-personal-data-protection-why-canada-should/

[224] C'est ce qu'on peut lire dans la réponse du Conseil de l'Europe au questionnaire de l'AMVP (PSWG3 - Privacy/Data Protection & Other Rights and Freedoms).
[225] Pour une liste complète des États non européens qui ont ratifié la Convention, voir : https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=Ryk2y1sX (consulté le 20 octobre 2020).
[226] G. Greenleaf, « How far can Convention 108+ 'globalise'? Prospects for Asian accessions » (2020) Computer Law & Security Review. Accès anticipé : https://doi.org/10.1016/j.clsr.2020.105414. Selon Greenleaf, les treize principaux avantages de l'adhésion à la Convention 108 sont les suivants : « (i) perspectives réalistes; (ii) aucune alternative réaliste; (iii) obligations volontaires; (iv) reconnaissance internationale des "pratiques exemplaires"; (v) exportations réciproques de données; (vi) normes modérées; (vii) normes minimales ; (viii) substitut de "liste blanche"; (ix) aide "d'adéquation"; (x) aide au développement; (xi) avantages commerciaux avec les exportations et les importations; (xii) avantages individuels avec des protections minimales; (xiii) aide aux organisations internationales ».
[227] Commission européenne, « Communication de la Commission au Parlement européen et au Conseil – Échange et protection de données à caractère personnel à l'ère de la mondialisation », COM (2017)7 final, p. 12.
[228] Rapporteur spécial de l'ONU sur le droit à la vie privée. « Rapport du Rapporteur spécial sur le droit à la vie privée », Soixante-treizième session de l'Assemblée générale de l'ONU [2018] UNSRPPub 11 (17 octobre 2018), alinéa. 117e).
[229] G Greenleaf, « How far can Convention 108+ "globalise"? Prospects for Asian accessions » (2020) *Computer Law & Security Review*. Accès anticipé : https://doi.org/10.1016/j.clsr.2020.105414 .
[230] Ibid., p. 19.
[231] Ibid., p. 19.
[232] Ibid., p. 4.
[233] Assemblé générale de l'ONU, Protocole facultatif se rapportant au Pacte international relatif aux droits civils et politiques, 19 décembre 1966, Organisation des Nations Unies, *Recueil des Traités de l'ONU*, vol. 999, p. 171, article 2.
[234] Par exemple, le PIRDCP de l'ONU reste une convention pertinente pour commencer ou continuer, mais il faut aussi tenir compte d'autres conventions, surtout quand il y a des dialogues ou des interactions (même de manière implicite) avec la protection des données et de la vie privée, comme la Convention relative aux droits de l'enfant, la Convention sur l'élimination de toutes les formes de discrimination à l'égard des femmes, etc.