LCCJTI+ : perspectives de mise à jour de la Loi concernant le cadre juridique des technologies de l'information (RLRQ c C-1.1) 2001 – 2023

Rapport final – 28 novembre 2023

Vincent GAUTRAIS
Pierre TRUDEL
Nicolas VERMEYS

Chaire L.R. Wilson
DROIT DES TECHNOLOGIES DE L'INFORMATION ET DU COMMERCE ÉLECTRONIQUE
UNIVERSITÉ DE MONTRÉAL

CENTRE DE RECHERCHE EN DROIT PUBLIC
C R D P

MISE EN GARDE

La présente étude a été réalisée à la suite d'un mandat confié aux auteurs par le ministère de la Justice du Québec en mars 2023[1]. Cela étant, les propos y contenus ne représentent que la seule position des auteurs et ne sauraient lier le ministère de la Justice du Québec ou ses représentants.

[1] La présente recherche a été grandement facilitée grâce au soutien de madame Sallia Zhang, étudiante à la Faculté de droit de l'Université de Montréal. Les auteurs remercient sincèrement Madame Zhang pour sa disponibilité et ses recherches très aidantes à la rédaction de la présente étude.

TABLE DES MATIÈRES

MISE EN GARDE ii

SOMMAIRE EXÉCUTIF 1

INTRODUCTION 17

PARTIE 1
LCCJTI+ : TENDANCES GÉNÉRALES EN DROIT DU NUMÉRIQUE

1.1 Tendances et état des faits 19

1.1.1 Tendances et risques 19

1.1.1.1 Mutation des risques 20

1.1.1.1.1 Les risques transcendent les frontières 20

1.1.1.1.2 Les risques concernent des acteurs professionnels ou non 21

1.1.1.1.3 Les risques concernant la sécurité et les libertés fondamentales 22

1.1.1.2 Augmentation des risques 22

1.1.1.3 Diversification des risques 23

1.1.1.3.1 Les objets 23

1.1.1.3.2 La viralité 23

1.1.1.3.3 Les capacités de reproduction à l'identique 23

1.1.1.3.4 Le rôle crucial des algorithmes 24

1.1.1.3.5 Les enjeux de souveraineté et d'interrégulation 24

1.1.1.3.6 Les capacités considérables de l'IA 24

1.1.2 Tendances et besoins 26

1.1.2.1 Identification des besoins initiaux 26

1.1.2.2 Sophistication des besoins 26

1.2 Tendances et état du droit 27

1.2.1 Tendances et densification des approches juridiques 27

1.2.1.1 Historique : du libertaire au libéral (1990–2010) 27

1.2.1.2 Densification progressive (2010 – …) 30

1.2.1.2.1 Influence de l'Europe: une densification assumée 30

1.2.1.2.2 Influence des États-Unis : une densification contrôlée 32

1.2.2 Tendances et spécificités des approches juridiques 34

1.2.2.1 Tendances vers plus de complexité 34

1.2.2.1.1 Complexité de l'objet d'analyse 34

1.2.2.1.2 Complexité du droit 36
1.2.2.2 Tendances vers plus de diversification des normes 37
1.2.2.3 Tendances diverses selon les spécificités culturelles 38
1.2.2.3.1 Selon la prévalence à utiliser des institutions 38
1.2.2.3.2 Selon les valeurs associées au Québec 39
1.2.2.3.3 Illustration 40
1.2.3 Tendances fonctionnelle et neutre des approches juridiques 40
1.2.3.1 Tendance fonctionnelle 40
1.2.3.1.1 Description de l'approche fonctionnelle 40
1.2.3.1.2 Approche fonctionnelle dans les démarches législatives récentes 42
1.2.3.2 Tendance et neutralité technologique 43

PARTIE 2
LCCJTI+ : MATIÈRES À CONSIDÉRER

2.1 LCCJTI + normativité 48
2.1.1 État des tendances 48
2.1.1.1 Tendances vers une augmentation du contrôle 48
2.1.1.1.1 Tendances plus directives 48
2.1.1.1.2 Tendances plus structurantes 52
2.1.1.1.3 Tendances plus prescriptives 55
2.1.1.1.3.1 Plus de prescription sur le fond 55
2.1.1.1.3.2 Plus de prescription sur la sanction 55
2.1.1.2 Tendances quant aux manières de réguler le technologique 57
2.1.1.2.1 Tendances participatives 57
2.1.1.2.1.1 Intérêts véritables d'une telle approche 57
2.1.1.2.1.2 Risques d'une participation mal contrôlée 59
2.1.1.2.1.3 Formalisation d'une approche participative 59
2.1.1.2.2 Tendances plus innovantes 64
2.1.1.2.2.1 Hypothèse des « bacs à sable réglementaires » (Sandboxes) 64
2.1.1.2.2.2 Hypothèse des « RegTechs » 68
2.1.1.2.2.3 Hypothèse de remise en cause des « silos » 71
2.2 LCCJTI + responsabilité 71
2.2.1 États des tendances 73
2.2.1.1 La valorisation des données massives 73
2.2.1.2 Les plateformes mettent le public à risque 74
2.2.1.3 Les manipulations, fraudes et hypertrucages 74
2.2.1.4 Le harcèlement 75

2.2.1.5 La publication non consensuelle d'images et d'images intimes 76
2.2.1.6 La publicité et les influenceurs 76
2.2.1.7 Tendances persistantes 76
2.2.1.8 L'impossibilité de contrôler ce à quoi accèdent les usagers 77
2.2.1.9 Ce qui est illégal hors ligne ne devient pas légal du seul fait que l'activité se déroule en ligne 77
2.2.1.10 Les intermédiaires ne peuvent être assimilés à des éditeurs mais ils sont en position de connaître les risques et de les minimiser 78
2.2.2 Réactions législatives 78
2.2.2.1 Réactions législatives et responsabilité en général 78
2.2.2.1.1 Les Principes de Manille sur la responsabilité des intermédiaires 79
2.2.2.1.2 Les principes de l'UNESCO 79
2.2.2.1.3 Le INFORM Consumer Act américain 81
2.2.2.1.4 La législation européenne sur les services numériques 82
2.2.2.1.5 La loi française sur les influenceurs en ligne 83
2.2.2.1.6 Les propositions de groupes de réflexion 84
2.2.2.2 Réactions législatives et responsabilité en intelligence artificielle 85
2.2.3 Propositions 85
2.2.3.1 Assurer la cohérence dans l'application des règles de droit 87
2.2.3.2 Des régulations sectorielles fonctionnant en réseaux 87
2.2.3.3 Protéger la liberté d'attention 88
2.2.3.4 Des devoirs de diligence 89
2.2.3.5 Obligations d'évaluer et de gérer les risques 89
2.2.3.6 L'imputabilité algorithmique 90
2.3 LCCJTI + identité 91
2.3.1 État des tendances 93
2.3.1.1 Tendance vers un abandon des approches initiales 93
2.3.1.1.1 Tendance vers un recul quant à la valorisation des signatures numériques 93
2.3.1.1.2 Tendance vers une reconfiguration de l'approche propre aux données biométriques 96
2.3.1.2 Tendance vers l'adoption d'une approche agnostique 98
2.3.1.3 Tendance vers une approche à la fois plus centralisée et décentralisée 99
2.3.1.3.1 Tendance vers l'adoption d'une identité numérique régalienne 100

2.3.1.3.2 Tendance vers une multiplication des fournisseurs d'identité 104
2.3.1.4 Absence de tendance relative à certains nouveaux développements 105
2.3.1.4.1 Les chaînes de blocs 105
2.3.1.4.2 L'hypertrucage 106

2.4 LCCJTI + sécurité 107
2.4.1 État des tendances 109
2.4.1.1 Tendance vers une analyse en silo des thématiques de sécurité 110
2.4.1.1.1 Tendance vers une approche sectorielle des thématiques de sécurité 110
2.4.1.1.2 Tendance vers une approche fonctionnelle des thématiques de sécurité 113
2.4.1.1.3 Tendance vers une approche technologique des thématiques de sécurité 114
2.4.1.2 Tendance vers une plus grande pénétration de l'analyse de risques dans les textes législatifs 115
2.4.1.3 Tendance vers une délégation de pouvoir aux organismes normatifs 116

CONCLUSION 118

BIBLIOGRAPHIE SOMMAIRE 122

SOMMAIRE EXÉCUTIF

Objet du rapport. L'objet de ce rapport est de faire état des tendances existant dans le monde au regard de l'encadrement des technologies et ensuite de suggérer ou évaluer lesquelles sont susceptibles de s'appliquer au Québec relativement à la *Loi concernant le cadre juridique des technologies de l'information* (ci-après « LCCJTI »). Ainsi, fort de ce constat et de ce survol, nous nous autorisons donc à une série de propositions qui pourraient agrémenter un texte qui, adopté il y a plus de 20 ans, a forcément un peu vieilli. Si le domaine du droit des technologies est large, tout comme le champ d'application de la LCCJTI, nous omettrons volontairement les questions de droit de la preuve qui ont déjà été traitées dans une étude de 2020 délivrée par le professeur Gautrais.

Nécessité d'un sommaire exécutif. Nous venons de le dire, le champ d'application de la LCCJTI est excessivement large. Aussi, eu égard à la transversalité du domaine des technologies, du sentiment partagé de la part des législateurs d'intervenir sur un domaine sujet à des changements d'importance, d'un phénomène de mode également, voire d'une urgence invoquée, notre rapport présente un nombre important de références législatives et doctrinales et, par le fait même, d'avenues qu'il a été nécessaire d'envisager. Aussi, il a été difficile de nous cantonner à la cinquantaine de pages initialement prévues. Afin de rendre notre propos plus accessible, peut-être pédagogique, nous avons cru bon de confectionner un sommaire exécutif capable de condenser l'essence du propos développé plus loin. Volontairement, ce sommaire sera dénué de notes de bas de page et nous invitons le lecteur à approfondir son appréhension du sujet avec l'étude qui le succède.

Plan. Conformément à une structure qui avait été arrêtée en juin 2023 avec l'équipe du MJQ, notre rapport se base dans une **première partie** sur les tendances que nous avons pu constater (Partie 1). Naturellement, elles concernent **en premier lieu** les technologies qui sont perceptibles à travers le monde (Section 1.1), mais aussi, **en second lieu**, le droit qui s'applique à elle (Section 1.2). Une fois cet état des lieux effectué, nous avons identifié dans une **seconde partie** (Partie 2) les grandes thématiques qui sont traitées dans la LCCJTI et qui forcément devront être envisagées au regard des changements préalablement constatés. Successivement, seront donc envisagées les questions de normativité (Section 2.1), de responsabilité (Section 2.2), d'identité (Section 2.3) et de sécurité (Section 2.4).

PARTIE 1 : LCCJTI+ – TENDANCES GÉNÉRALES EN DROIT DU NUMÉRIQUE

1.1 Tendances et état des faits

Si les technologies font tellement parler d'elles, c'est que de façon perçue ou réelle, elles donnent lieu à la survenance de nouveaux risques qui eux-mêmes exigent des réponses législatives capables de remplir de nouveaux besoins.

1.1.1 Tendances et risques

Mutation des risques. En seulement 20 ans, une véritable mutation des risques est apparue. Alors qu'au début du siècle, on percevait les risques technologiques au regard des seules transactions qui

étaient désormais rendues possibles, un éclatement des hypothèses à risques est perceptible. Tous les champs d'activité sont concernés d'autant qu'un décloisonnement des frontières habituelles s'opère. Ce décloisonnement concerne **en premier lieu** les frontières géographiques qui deviennent de plus en plus poreuses, les technologies se déployant globalement et même l'encadrement, qu'il soit légal ou technique, donnant lieu à des inspirations mondiales. Les frontières se fragilisent aussi, **en deuxième lieu**, dans la distinction autrefois plus aisée entre professionnels et individus. Avec la multiplication des plateformes, et leur puissance accrue, les individus détiennent, d'une part, des statuts distincts cumulant parfois des rôles de consommateur, de citoyen, d'individu. Ils sont aussi, d'autre part, avec l'économie dite collaborative, des entrepreneurs, des diffuseurs de contenus, des vendeurs, des prestataires de services. On est donc très loin de la structure économique sur laquelle les dispositions relatives à la responsabilité (articles 22 et ss. LCCJTI) avaient pris fondement. **En troisième lieu**, ces mutations ont forcément un effet direct sur les catégorisations que le droit ne manque pas d'apporter. D'autant que ces changements créent des zones de contact entre les disciplines qui n'avaient pas été envisagées. À titre d'exemple, avec les médias sociaux, on est confronté à de nouveaux équilibres entre liberté d'expression et atteinte à la réputation.

Contrôle des risques difficiles. La rapidité de l'évolution des phénomènes fait en sorte qu'il est parfois difficile de les encadrer. Le phénomène *AirBnB*, par exemple, a obligé la mise en place rapide de règles dont le contrôle n'est pas toujours aisé à effectuer par les institutions responsables. À certains égards, on se trouve parfois dans des situations où une certaine « tolérance » existe vis-à-vis de nouveaux risques qui ne sont pas toujours maîtrisés.

Imputabilité des risques. Une tendance importante est de laisser les risques sur les épaules de l'utilisateur, et ce, en dépit du fait qu'il n'est pas toujours bien armé pour ce faire. À titre d'exemple, une portée juridique importante est tributaire du consentement que l'usager fait en étant membre de Facebook; il doit maîtriser l'usage de ses données; paramétrer la manière dont ces dernières sont utilisées. Une réflexion s'impose donc sur ce rôle important dévolu, souvent, à la « partie faible ».

Diversification des risques. Sans les citer tous, au niveau des grandes tendances en matière de risques, il est possible d'en lister un certain nombre qui montre la diversification du phénomène. Ainsi, on peut identifier :

1) les objets connectés qui deviennent désormais des producteurs croissants de données sur lesquels il est difficile d'avoir le contrôle;
2) la viralité inhérente aux environnements en réseaux génère de nouveaux risques étant donné la disponibilité accrue de l'information;
3) au-delà de la capacité de reproduction qui avait été considérée en 2001 par la LCCJTI, la donne change avec la capacité de trucage qui est désormais telle que cela remet en cause la hiérarchie entre copie et original;
4) la généralisation des algorithmes qui, du fait de leur capacité de décision, peuvent se substituer à une décision humaine, et ce, sans que l'on sache toujours, par manque de transparence, comment la décision est prise;
5) de manière plus générale, l'intelligence artificielle et notamment l'apprentissage profond qui multiplie les capacités de calculs, là encore avec un niveau d'opacité accentué;
6) la pluralité des couches normatives tant juridique, éthique que technique nous invite à nous interroger sur la perte de souveraineté des États qui perdent le contrôle, se faisant

concurrence par d'autres instances ne disposant pas de la même légitimité (industrie, standards techniques, etc.);
7) etc.

1.1.2 Tendances et besoins

Besoins initiaux. Même si ce n'est pas l'objet du rapport, il importe au départ de bien identifier les objectifs pour lesquels la LCCJTI a été adoptée en 2001 : **en premier lieu**, elle avait vocation à favoriser le commerce électronique, tentant de « lisser » les éventuels irritants juridiques que l'« ancien droit » pouvait causer au « nouveau monde ». On peut par exemple penser à l'article 5 LCCJTI. **En deuxième lieu**, il s'agissait d'identifier certaines balises, notamment en matière de sécurité, afin de guider les acteurs. Même si ce fut parfois jugé trop minimaliste, l'article 6 tente de préciser en quoi consiste le critère d'intégrité. **En troisième lieu**, et de façon assez innovante, la LCCJTI a intégré à plusieurs reprises des considérations liées aux libertés publiques, ayant bien conscience que les technologies étaient susceptibles de les affecter. On peut par exemple citer les articles 2, 29, 40 à 45, des dispositions qui ont, par exemple, totalement vocation à s'appliquer sur les questions actuelles d'intelligence artificielle.

Sophistication des besoins actuels. Si plusieurs des dispositions sont donc toujours applicables, il n'en reste pas moins vrai qu'une actualisation est requise au regard des nouveaux besoins que la nouvelle réalité nous oblige à considérer. Nous souhaitons en lister quelques-uns :

1) le numérique altère les **rapports de force**, certaines entités devenant plus fortes et d'autres plus faibles. Le droit doit donc « corriger » ces altérations et déterminer l'équilibrage qu'il considère comme étant adéquat;
2) les technologies génèrent de nouvelles **opacités**. Si cette problématique a été identifiée dès le début du numérique, elles sont accentuées récemment notamment avec de nouveaux outils tels que, par exemple, l'intelligence artificielle ou les chaînes de blocs.
3) ces deux précédents points, forcément, vont avoir une incidence sur les **responsabilités** telles que décrites dans la LCCJTI, et ce, au regard de la notion de contrôle prédominante dans la LCCJTI qui détermine le niveau de responsabilité selon la capacité des acteurs d'en avoir ou pas. Désormais, de nombreuses plateformes disposent d'un contrôle puissant sur les activités des usagers;
4) de nouvelles **discriminations** apparaissent et il importe de s'interroger sur la pertinence de développer de nouveaux textes législatifs capables de densifier les obligations des acteurs;
5) de la même manière, il importe de se questionner sur l'importance d'encadrer la généralisation des **décisions automatisées**, au-delà de ce qui prévaut déjà dans la LCCJTI (art. 35) ou dans la nouvelle Loi 25;
6) enfin, nous croyons important de disposer d'une **normativité** capable d'agir de façon **proactive** et en mesure de répondre rapidement à l'évolution permanente du contexte technologique. Une normativité en réseau pour un droit en réseau.

1.2 Tendances et état du droit

1.2.1 Tendances et densification des approches juridiques

(1990 - 2010) Début libertaire. Relativement à l'état du droit, il importe de rappeler, après un survol historique, que le droit de l'Internet a suivi la tendance libertarienne qui caractérisait l'outil de communication dans les années 1990. Que ce soit en matière de responsabilité, de contrat, de vie privée, de plateformes, de normativité, on ne souhaitait pas trop imposer d'obligations aux acteurs et permettre ainsi à cette industrie naissante de se développer. Cette tolérance se retrouve dans la jurisprudence et même dans le récent traité « Canada – États-Unis – Mexique » (ACEUM).

(2010 - …) Tendance plus exigeante. La donne a néanmoins changé il y a quelques années à travers le monde, on a aperçu un peu partout des lois se multiplier et hausser en contrainte. Si tendance il y a, il faut néanmoins constater une différence assez sensible entre l'Europe et l'Amérique.

Approche européenne. Clairement, l'Europe opte pour une approche interventionniste et multiplie des textes qui imposent des obligations parfois assez lourdes aux différents acteurs. Sans les citer toutes, on peut citer un règlement sur l'identité numérique (2014), le RGPD sur la vie privée (2016), deux règlements en 2022, respectivement sur le contrôle des services (DSA) et des marchés (DMA) et récemment un règlement sur l'intelligence artificielle (2023). Cette floraison textuelle s'apparente à un phénomène qui a été qualifié d'« effet Bruxelles » et selon lequel l'Europe tente d'influencer quant aux manières de réguler les technologies en imposant un « standard » élevé de contrainte. Fait important, la mise en place de ces textes s'opère avec une structure administrative, tant européenne qu'à l'échelle nationale, relativement conséquente, des entités étant créées pour surveiller l'application des règles.

Approche canadienne. Au Canada, la situation varie selon les disciplines. Si un texte récent est venu encadrer les plateformes de communication en ligne (C-18), le numérique n'a pas donné lieu à beaucoup d'adaptation législative. Certes, il y a eu notamment une modification de la *Loi sur le droit d'auteur* (2012), un texte pour contrer les pourriels (2017), des adaptations ponctuelles en protection des renseignements personnels, il manque des textes majeurs qui viennent préciser et augmenter les obligations des acteurs. Depuis près de quatre ans, un projet de loi en matière de protection des renseignements personnels existe (C-11 puis C-27) auquel s'est greffée en 2022 une partie dédiée à l'intelligence artificielle. Ce dernier texte demeure nébuleux et s'il traduit cette même tendance de densification des règles, beaucoup de dispositions s'avèrent imprécises, notamment relatives à l'intelligence artificielle, qui seront précisées par un règlement ultérieur. D'ailleurs, sur cette question, le 30 septembre 2023, le ministre Champagne a préconisé l'adoption d'un Code de conduite volontaire.

Approche états-unienne. Aux États-Unis, si un discours politique semble manifester la même préoccupation pour contrôler les activités technologiques, aucun texte d'envergure n'est venu compléter le corpus de règles existant. En effet, les seules voies entrevues concernent soit des projets de lois (intelligence artificielle (2022), blockchain (2022)), dont aucun n'a été adopté, soit des études gouvernementales (White Papers), soit des normes informelles telles que des listes de principes ou lignes directrices (2023). Assurément, cet État est moins enclin à contraindre trop intensément une industrie qui provient de son propre pays.

1.2.2 Tendances et spécificités des approches juridiques

Complexité des technologies. La première caractéristique que nous croyons importante de signaler est que les technologies que nous cherchons à appréhender décèlent un haut niveau de complexité. Outre l'opacité déjà signalée, nous sommes face à un monde évolutif et il importe à une loi traitant des technologies comme la LCCJTI d'avoir une faculté d'adaptation et de résister au temps. À certains égards, la LCCJTI remplit assez bien cet objectif et trois illustrations peuvent être données. **En premier lieu**, le terme même de « **technologie** » qui est central dans la LCCJTI a bien vieilli et traduit toujours aussi bien la réalité numérique. En effet, le terme est inclusif et comprend ce qui n'est pas « physique », « analogique ». Il peut donc intégrer les nouveautés qui ne manquent pas d'apparaître. **En deuxième lieu**, une partie de la LCCJTI (le chapitre 2) avait tenté de considérer l'ensemble des opérations que l'on pensait possible et quatre d'entre elles ont été spécifiquement encadrées, soit le transfert (17 et ss.); la conservation (19 et ss.); la consultation (23 et ss) et la communication (28 et ss.). Or, certaines d'entre elles n'avaient pas été envisagées alors qu'il faudrait qu'elles le soient désormais. Par exemple, le fait de « faire parler les données », comme le fait l'intelligence artificielle, est une activité qui demande un cadre; cadre dont on ne pouvait suspecter l'importance en 2001. Il est donc important de prévoir un encadrement de ce que nous appelons l'utilisation ou mieux encore le « traitement » des données. Un traitement qui compléterait le spectre des opérations qui doivent être encadrées, nous laissant croire que la LCCJTI soit un socle naturel pour considérer les questions entourant l'intelligence artificielle. **En troisième lieu,** s'il est vrai qu'en 2023, on parle généralement de « donnée » et de la nécessité d'un droit de la donnée, il n'y a pas de contradiction avec la notion de « document » qui constitue la composante centrale autour de laquelle la LCCJTI s'est construite. En effet, le document est une information portée sur un support (art. 3). Or, l'information, sous-composante du document, peut être assimilée à une donnée, la première étant structurée (comme le dit l'article 3) alors que la seconde est un élément brut.

Complexité du droit. Cette complexité technologique se traduit forcément dans le droit. Sans être exhaustif, nous aimerions en citer quelques raisons. **En premier lieu**, la nouveauté est source d'incertitude du fait de l'absence de recul sur les sujets à traiter. **En deuxième lieu**, plusieurs technologies présentent une rupture avec les structures traditionnelles (comme la chaîne de blocs) bouleversant les modes habituels de contrôle. **En troisième lieu**, il est commun de réguler le technologique avec une pluralité de normes qui se superposent : la loi réfère à des décrets qui réfèrent à des normes techniques, elles-mêmes exigeant habituellement de rédiger des documentations internes. Ce *modus operandi* n'est pas si maîtrisé d'autant que des doutes existent sur l'existence et le contenu de ces normes. **En quatrième lieu**, si la réflexion autour de l'encadrement des technologies s'opère au niveau mondial, il existe des différences « culturelles » entre les pays. Ces distinctions peuvent se matérialiser au niveau de la substance : à titre d'exemple, le droit à l'oubli dans la Loi 25 n'a pas la même portée que le RGPD dont elle s'inspire. Également, il est autorisé au Canada, sauf exception, de laisser les noms des parties à un procès dans les banques de données juridiques, alors qu'en Europe les noms des parties sont « caviardés », la vie privée surmontant le principe de la publicité des débats judiciaires. Sur le plan institutionnel, il existe aussi une différence notable, les européens ayant plus tendance à exiger l'intervention d'une entité étatique. Que ce soit en matière d'identité numérique (Règlement eIDAS (2014)) ou d'intelligence artificielle (Règlement sur l'IA (2023)), les textes européens imposent la présence d'un cadre administratif qui semble moins systématique au Canada.

1.2.3 Tendances fonctionnelle et neutre des approches juridiques

Approche fonctionnelle. La LCCJTI a été forgée sur deux principes fondateurs. Le premier est celui de l'approche fonctionnelle selon lequel on doit construire le droit pour le numérique en se basant sur les fonctions qui avaient été identifiées pour le papier. Ce principe notamment véhiculé dans les travaux de la CNUDCI (Commission des Nations unies pour le droit du commerce international) fonctionne donc comme un « calque » que l'on utilise pour encadrer la nouvelle réalité. Concrètement, il importe lorsque c'est possible de rédiger les lois d'une manière qui puisse s'appliquer à la fois à différents supports et à de nouvelles technologies. À titre d'exemple, les articles 40 et ss. de la LCCJTI sont susceptibles de s'appliquer à la nouvelle réalité des caméras dites intelligentes que certaines entreprises veulent notamment exploiter dans les pharmacies pour lutter contre le vol à l'étalage. En effet, les dispositions qui avaient en tête les questions de biométrie en 2001 évoquent non pas ce dernier terme qui réfère à une empreinte de doigt, une forme de la main, l'iris d'un œil, mais utilisent plutôt le terme de « document technologique qui présente une caractéristique personnelle » (art. 41) ou même « banque de caractéristique » (art. 45). Après, si le principe est solide et semble toujours d'actualité, il demeure parfois difficile à opérationnaliser, tant la comparaison avec l'analogique est parfois délicate. La CNUDCI relève en effet des hypothèses, comme en matière d'identité numérique où l'équivalent papier n'existe pas. Il en va de même, par exemple, du phénomène des plateformes où il est difficile d'effectuer une comparaison.

Neutralité technologique. Le second principe fondateur dans la LCCJTI, tout comme dans la plupart des lois sur le numérique, est celui de la neutralité technologique. Par cette expression, on entend le fait d'une loi de ne pas traiter, dans la mesure du possible, d'une technologie en particulier mais davantage d'un cadre plus général. D'ailleurs, en dépit de son nom, la LCCJTI s'applique à la fois au papier et au technologique. Beaucoup de lois anciennes comme récentes se réclament de cette approche. Pourtant, en 2001 comme en 2023, des lois vont à l'encontre de ce principe. Par exemple, la LCCJTI possède des dispositions spécifiques sur les infrastructures à clés publiques (art. 46 à 62) ce qui est une entorse à ce principe. De la même manière, on voit les lois sur l'intelligence artificielle ou les chaînes de blocs fleurirent çà et là, ciblant ces technologies en particulier. Un vrai débat plus conceptuel existe donc sur le fait de savoir si l'on doit choisir une option plus neutre technologiquement ou au contraire opter pour une « discrimination technologique ». D'une manière générale, les lois neutres tendent à être perçues comme résistant mieux au temps (*future proof*), alors que les lois discriminantes permettent une meilleure adaptation aux faits (*increased tailoring*). D'une manière générale, nous croyons que si la neutralité technologique est un principe par défaut, elle souffre d'exception, notamment lorsque des éléments de spécificités apparaissent. Cette question vaut par exemple pour l'intelligence artificielle où, comme avancé précédemment, la question du traitement des données est susceptible de s'immiscer dans les opérations déjà prévues dans la LCCJTI. Il nous semble donc que cette loi pourrait être un « réceptacle » approprié pour traiter de cette question. Après, cela n'empêcherait pas un traitement technologiquement spécifique pour certaines questions plus particulières comme les voitures autonomes ou l'utilisation de l'intelligence artificielle dans un contexte scolaire, du fait de spécificités plus en lien avec des problématiques spéciales, des acteurs et des instances de contrôle particuliers.

PARTIE 2 – LCCJTI+ – MATIÈRES À CONSIDÉRER

2.1 LCCJTI + Normativités

Comment réguler ? La première question que nous souhaitons envisager concerne l'encadrement général des technologies : comment fait-on ? En se basant sur le survol mondial qui constitue le cœur du mandat, nous croyons apercevoir des directions constatées dans les tendances recherchées qui peuvent se matérialiser de cinq façons différentes.

2.1.1 Tendances plus directives

Tendance vers plus d'intervention. La LCCJTI avait instauré plusieurs possibilités pour rendre la loi dynamique et adaptable aux circonstances nouvelles. Ainsi, dès le départ, elle autorise d'adopter des décrets (art. 8), des règlements (art. 69) et le Comité d'harmonisation (art. 63 et ss.) était là pour « nourrir » ce besoin d'adaptation et de complétude normative. En 20 ans, bien peu fut fait. Ceci semble contraire à une tendance récente selon laquelle les États cherchent à se mobiliser pour encadrer davantage, et ce, même en tenant compte de la différence entre l'Europe et l'Amérique, la seconde étant moins interventionniste que la première. Comme mentionné plus tôt, au-delà du degré d'intervention, se pose la question de savoir si l'encadrement d'une technologie implique une approche concernée, entre plusieurs instances, ou au contraire une démarche plus sectorielle. Neutralité versus spécificité technologique, les deux démarches s'aperçoivent. Si le projet de loi C-27 au fédéral entend proposer une loi dédiée à l'intelligence artificielle, la démarche anglaise, par exemple, entend opérer un traitement concerté entre plusieurs institutions existantes.

Comité d'harmonisation. Cette inclinaison a davantage de direction et nous amène à évaluer la réponse institutionnelle que chaque cadre légal prévoit généralement. Face à une technologie, quelle instance doit être mise en place pour favoriser l'application de la loi et quels sont ses pouvoirs ? Relativement à la LCCJTI, il importe de considérer le rôle dudit Comité d'harmonisation dont les fonctions ont été ajustées en 2021 par le projet de loi 6 (*Loi sur le ministère de la Cybersécurité et du Numérique*). Un rôle qui a été étendu et qui est moindrement associé à la production de normes techniques et davantage à tout « autres documents » comme des guides, des modèles, des lignes directrices, etc. Un domaine d'application qui semble aussi très inclusif, l'expression « utilisation des technologies » autorisant désormais de considérer les sujets du jour comme les chaînes de blocs ou l'intelligence artificielle, notamment. Nous croyons donc qu'au-delà de l'harmonisation, le comité pourrait jouer un rôle plus englobant, comme cela se fait avec le DSA en Europe (art. 61). Un rôle que nous qualifions d'« animation normative ». Également, ce Comité d'harmonisation pourrait servir de dialogue inter-institutionnel, la transversalité de certaines technologies faisant en sorte que plusieurs instances pourraient être intéressées par les mêmes problématiques (comme la Commission des droits de la personne, la Commission d'accès à l'information, l'Office de la protection du consommateur, etc.). D'ailleurs, relativement à ce rôle de nécessaire relation avec d'autres instances du gouvernement du Québec, nous constatons que la place du Comité d'harmonisation de la LCCJTI n'est pas clairement déterminée au regard des chevauchements inévitables qui prévalent avec le comité équivalent et mis en place par la *Loi sur le ministère de la cybersécurité et le numérique* (art. 9).

2.1.2 Tendances plus structurantes

De façon très proche de ce précédent point, nous apercevons aussi dans les textes étudiés une tendance vers plus de structuration. Celle-ci se manifeste **en premier lieu** dans le dialogue internormatif, d'abord auprès des normes informelles (code de conduite, lignes directrices, etc.), mais aussi au niveau applicatif, les PME étant souvent très démunies pour élaborer de tels textes. Si l'on souhaite que les technologies soient l'affaire de tous, et non pas les seules entreprises d'envergure, une aide est requise; aide qui ne peut venir que d'un organisme légitime qui viendrait produire ou adouber un modèle existant. **En deuxième lieu**, cette structuration implique généralement un soutien financier afin que l'institution en charge du comité puisse atteindre son niveau d'ambition. S'il est difficile d'accéder à l'étranger aux budgets des instances en charge de ce rôle vers plus de structuration, on peut citer la hausse budgétaire significative de la Commission d'accès à l'information à la suite de l'augmentation de ses prérogatives avec la Loi 25 ou le budget alloué par le fédéral pour la rédaction de normes en matière d'intelligence artificielle par le Conseil canadien des normes. **En troisième lieu**, il semble nécessaire qu'une collaboration s'opère entre des instances qui, si elles cherchent à défendre les intérêts de personnes avec des statuts différents (consommateur (LPC), individu (vie privée), citoyen (charte), etc.), concernent en bout de ligne les mêmes personnes. Cette collaboration est également requise afin d'optimiser les ressources d'instances qui gagneraient à s'allier avec d'autres. Cette tendance s'aperçoit en Europe pour lutter contre les GAFAM; elle est également perceptible au Canada lorsque des instances en matière de vie privée unissent leurs forces pour lutter contre des entreprises contrevenant aux règles (par exemple, l'affaire *Clearview AI* (2021)).

2.1.3 Tendances plus prescriptives

Sanctions en hausse. La présente partie 2 souligne de manière générale une tendance vers une hausse des obligations de la part des différents acteurs, et ce, tant sur les questions de responsabilité (2.2), d'identité (2.3), et de sécurité (2.4). D'ailleurs, le moyen de souligner cette tendance est de constater dans plusieurs domaines de droit une hausse significative de sanctions pécuniaires d'importance. Initiées par le RGPD en 2016, l'Europe a généralisé des pénalités pouvant aller jusqu'à 4 ou 5 % du chiffre d'affaires mondial de l'entreprise. L'Europe a étendu cela en matière de concurrence (DMA), de responsabilité des plateformes (DSA), d'intelligence artificielle (AIA). Et l'influence est sensible tant au Québec (Loi 25), au Canada (C-27) et dans d'autres juridictions, comme en Chine, à l'exception des États-Unis pour le moment.

2.1.4 Tendances plus participatives

Tendance vers plus de participation. De plus en plus, les lois observées tendent à intégrer un phénomène de participation qui se manifeste de différentes manières. **En premier lieu**, et comme déjà dit, les lois tendent à se limiter à de grands principes obligeant les acteurs à se baser sur des normes communautaires (comme des standards techniques, des lignes directrices, etc.) qui eux-mêmes réfèrent à des documentations internes. **En second lieu**, il existe plusieurs lois ou autres textes qui prennent le soin de s'assurer que la population participe à l'élaboration ou à l'application des règles. En effet, des lois (comme la *Loi française sur la république numérique* (2019) ou le AIA (2023)), des textes communautaires (comme la Déclaration de Montréal (2018)), même des traités (comme des accords entre le UK et la Nouvelle-Zélande (2022)) cherchent à opérer des consultations de la part des parties prenantes. Cette manière de faire est en revanche parfois

critiquée, le phénomène étant vu comme un moyen pour les États de ne pas s'investir dans l'élaboration des règles.

Formalisation de cette participation. Aussi, pour s'assurer de la légitimité de telles manières de faire, il importe de formaliser l'intervention des parties concernées qui peut se matérialiser différemment. En voici quelques illustrations. **En premier lieu**, de façon générale, il est possible de faire des consultations soit en invitant le grand public, soit des experts sur la question. L'important est que celles-ci soient réelles et significatives et non une façade utilisée par l'institution responsable pour justifier une position.

Lanceurs d'alerte. **En deuxième lieu**, une façon de faire est de faciliter toute personne qui aurait été témoin d'un problème de mise en application de la loi. Aussi, plusieurs juridictions ont légiféré sur la protection des lanceurs d'alerte. L'idée est simple : outre le fait de soulever des failles dans un système, cela permet de canaliser le « coulage » d'information plutôt qu'une divulgation qui serait faite directement au grand public. Le constat que l'on peut faire est, d'une part, que la mise en place d'une telle mesure peut exiger une structure administrative assez lourde. D'autre part, à l'échelle québécoise, il existe déjà plusieurs cadres pour organiser la dénonciation par des individus et en dépit de certaines spécificités liées au numérique (comme l'opacité), il ne nous est pas apparu nécessaire d'en mettre une en place qui soit dédiée à la LCCJTI.

Hackeurs légaux. **En troisième lieu**, et toujours selon cet objectif de faire participer plus de monde, nous avons aperçu quelques lois souhaitant favoriser et donc protéger les hackeurs dites « éthiques ». Au-delà du fait que cette démarche a tout de même été assez rarement entreprise, il faut remarquer que dans le contexte québécois, d'une part, il existe un enjeu criminel qui ne relève pas de la province et, d'autre part, il importe de s'interroger sur la pertinence de formaliser ce statut dans une loi. En effet, au-delà des chevauchements possibles avec le droit de la responsabilité civile (et notamment l'article 1457 C.c.Q), il est possible de développer une démarche plus « éducative » sans forcément introduire un changement législatif.

2.1.5 Tendances plus innovantes

Bacs à sable réglementaires. Sans volonté d'exhaustivité, nous avons cru bon d'identifier minimalement deux techniques réglementaires aperçues çà et là dans notre analyse des lois liées au numérique. La **première** concerne les bacs à sable réglementaires, à savoir, un projet expérimental temporaire où l'on teste un cadre réglementaire en invitant des parties prenantes à participer à une réflexion. Très à la mode, cette technique réglementaire ne bénéficie pas encore de beaucoup de recul, et ce, même si on la trouve dans un assez grand nombre de lois, notamment dans le domaine des « fintechs », des voitures autonomes, de l'intelligence artificielle. Selon l'approche fonctionnelle précitée, ils permettent d'établir un équilibre entre deux fonctions quelque peu contradictoires, soit la protection et l'innovation. Cet équilibre est notamment souvent vu comme étant difficile à déterminer pour les plus petites structures qui bénéficient de moins de moyens et sont donc plus facilement perdues. Les bacs à sable réglementaires sont donc aussi un moyen d'améliorer la concurrence.

Garantir les bacs à sable réglementaires. Paradoxalement, cet outil se trouve un peu partout et, notamment, tant dans des textes américains qu'européens (comme le AIA (2023)). En revanche, les textes qui en parlent n'établissent pas toujours des garanties pour compenser l'informalité du

processus. Un certain nombre d'entre elles peuvent néanmoins être identifiées tel que l'institutionnalisation de son processus, les modalités de sélection, la manière de générer des consensus et de gérer les dissensus, la transparence, les ressources allouées, etc.

« Regtechs ». Un **second** procédé que nous croyons important de citer est le phénomène des « regtechs » correspondant à des outils généralement logiciels qui permettent à une institution (souvent une banque ou autre instance dans le monde de la finance) d'automatiser sa reddition de compte. Face à la hausse croissante de cette obligation d'auto-proclamation ou de documentation interne, l'idée est venue de développer des applications technologiques capables de dévoiler la diligence des acteurs. Si l'idée est intéressante, le procédé fait encore l'objet de critiques telles que le fait que peu de lois ne soient intervenues (mais davantage des études ou documents internes d'organismes de contrôle); la complexité des procédés rend l'explicabilité délicate; le manque d'uniformité des approches; la complexité rend les plus grosses structures plus aptes à les intégrer. De ce néologisme pourtant récent est depuis peu apparue la notion de « SupTech », à savoir des outils technologiques pour faciliter la supervision. Généralement associée à un organisme de contrôle, elle permet à ce dernier de rendre disponible des moyens pour mieux se conformer aux règles applicables. Au-delà du monde de la finance, quelques exemples peuvent être trouvés en matière de protection des renseignements personnels ou de l'intelligence artificielle.

Éviter les silos. Enfin, et sans que cela ne soit développé, nous voulons seulement faire état du fait que de façon unanime, il est reconnu que les pratiques en silos, sans tenir compte d'une approche plus globale, sont un défaut encore malheureusement constaté.

2.2 LCCJTI + responsabilités

La LCCJTI en 2001 a mis en place, comme partout ailleurs dans le monde, différents régimes limitant la responsabilité des acteurs techniques (voir 1.2.1.1), et ce, que ce soit pour les services 1) de conservation (hébergeurs); 2) de référence (outils de recherche); 3) de transmission; 4) de garde (conservation avec sécurité). Globalement, ce régime de responsabilité est basé sur la connaissance du caractère illicite de l'activité et sur la capacité de contrôle de l'intermédiaire.

2.2.1 État des tendances

Données massives. Comme mentionné plus tôt, le contexte des plateformes mondiales actuelles a complétement changé depuis 2001 du fait de leur toute-puissance et de la capacité de contrôle dont elles disposent. Les modèles d'affaires sont désormais basés sur la valorisation de quantités astronomiques de données notamment personnelles.

Risques également collectifs. Mais ces risques ne sont pas seulement individuels; ils concernent aussi la protection du public dans son ensemble face aux menaces à des droits collectifs tels que l'information du public face à un contrôle de celle-ci de plus en plus assuré par des multinationales.

Manipulations. L'hypertrucage est depuis quelques années un autre risque de plus en plus évoqué. Accessible à tous, de faux profils apparaissent et peuvent être utilisés par des personnes mal intentionnées, et ce, même si les lois générales s'appliquent à eux.

Harcèlement. Certains risques, comme le harcèlement, visent de surcroît plus particulièrement certaines catégories de personnes, comme les femmes, et si les règles générales sont applicables, il n'est pas toujours aisé d'assurer leur respect.

Publication non consensuelle. C'est la raison pour laquelle dans certains cas des lois spécifiques sont intervenues. On peut notamment penser au *Intimate Images Protection Act* de la Colombie-Britannique ou, au Québec, à l'article 28.1 de la *Loi sur la protection des renseignements personnels dans le secteur privé* dès lors qu'une publication va à l'encontre de la loi ou d'une ordonnance judiciaire.

Publicité et influenceurs. Comme souvent au Québec, il y a néanmoins une faveur vis-à-vis des règles générales. Aussi, relativement aux risques associés aux activités des influenceurs, ce sont davantage des lois telles que la *Loi sur la protection du consommateur* qui sont susceptibles de s'appliquer.

Trois tendances persistantes. Enfin, il est possible d'identifier trois tendances sur lesquelles il faut s'interroger. La **première** est de se demander si l'on doit continuer de limiter la responsabilité des plateformes sur la base que ce ne sont pas elles qui accèdent à l'information source à problème. En effet, les modalités de contrôle ont changé. La **deuxième** est la croyance trop souvent partagée selon laquelle les activités numériques sont moins sources d'infraction que celles similaires faites hors ligne. Après, le contexte différent rend le partage entre ce qui est prohibé et la liberté d'expression parfois délicat; un partage qui ne doit être effectué que par un ou une juge, ce qui est parfois difficile à faire eu égard au temps que ce processus demande, alors que les réseaux exigent une réactivité plus grande étant donné les dommages possibles. Finalement, la **troisième** tendance concerne le fait que les intermédiaires ne peuvent être assimilés à des éditeurs, n'ayant pas l'intention d'exercer un contrôle sur l'information. Ceci est d'ailleurs clairement reproduit dans l'*Accord Canada-États-Unis-Mexique* (ACEUM). Pourtant, certaines législations sont venues densifier les obligations des plateformes.

2.2.2 Réactions législatives

Responsabilité en croissance en général. Le premier type de réaction législative concerne la responsabilité en général. Notre survol des législations montre un spectre très étendu des possibilités quant à l'équilibre difficile entre les plateformes et les usagers. Une tendance lourde vise néanmoins à préciser les rôles. Sur le plan international, on peut d'abord citer les *Principes de Manille* qui, en 2015, élaborent six principes généraux qui, assurément, sont déjà de mise dans le droit actuel du Québec (tel que la proportionnalité, la prévalence de procédure judiciaire, la transparence, etc.). En 2022, les Principes de l'UNESCO constituent cinq principes de base qui précisent cet équilibre. Nous souhaitons rapidement les citer : ainsi les plateformes doivent :

- respecter les droits humains;
- respecter les normes internationales en droit de la personne;
- respecter les règles de transparence;
- mettre des informations à disposition du public;
- être imputable.

Sur le plan national, il importe de citer d'abord le *INFORM Consumer Act* adopté aux États-Unis en juin 2023. Appliquée par le *Federal Trade Commission* (FTC), cette loi oblige les marchés en

ligne à vérifier et partager de l'information sur les tiers vendeurs et notamment ceux qui ont de gros volume de transactions. Ces derniers sont assujettis à certaines autres obligations de mise à jour et de permettre de signaler facilement les comportements suspects. Sinon, l'Europe est assurément l'espace géographique où les obligations des plateformes ont été les plus densifiées. Le DSA de 2022 oblige notamment les très grandes plateformes à identifier et gérer les risques de manipulation et d'information. Ces dernières devront mettre en place de nouvelles politiques qui devront être auditées. L'obligation d'information des utilisateurs sera augmentée et ils auront la possibilité de se soustraire au profilage et autres méthodes publicitaires. De façon similaire, une loi française adoptée en juin 2023 vise « à encadrer l'influence commerciale et à lutter contre les dérives des influenceurs sur les réseaux sociaux ». Une définition d'influenceur est ainsi donnée et la loi oblige les plus importants à divulguer notamment les conditions de rémunération. Un régime de responsabilité solidaire est aussi mis en place entre l'influenceur, son agent et l'annonceur. Notons enfin que la promotion de certains biens ou services est interdite (services financiers, chirurgie esthétique, nicotine, jeux d'argent, etc.). Notons enfin que la *Commission canadienne de l'expression démocratique* a en 2021 mis de l'avant certaines propositions afin de protéger l'intégrité des échanges en ligne. Parmi les avenues envisagées, une responsabilité de principe est proposée qui vaudrait tant pour les plateformes de réseaux sociaux que pour les moteurs de recherche. Pour assurer la mise en place de texte, un organisme public est requis.

Responsabilité en croissance dans le cas particulier de l'intelligence artificielle. Que ce soit dans des lois (ex. : AIA), des projets de lois (ex. : C-27), des textes de nature informelle (ex. : Déclaration de Montréal), une tendance forte est de baser l'encadrement de l'intelligence artificielle sur les risques qu'elle suscite.

2.2.3 Propositions

Actions possibles. Au regard des dispositions existantes, nous croyons qu'une approche en trois temps est requise : 1) d'abord, l'article 22 peut être maintenu sous réserve de préciser les modalités de la connaissance; 2) ensuite, une instance viendra assurer la conformité de ces conditions, notamment relativement aux enjeux liés à l'intelligence artificielle; 3) un traitement techno-spécifique peut être envisagé lorsque la question présente un certain niveau de spécificité (ex. : les voitures autonomes).

Fonctions à satisfaire. En mettant en place cette approche en trois temps, il convient, **en premier lieu**, d'assurer une cohérence entre la LCCJTI et les lois existantes, conformément à l'article 1 LCCJTI, et notamment une équivalence des règles applicables en ligne et hors ligne. **En deuxième lieu**, une collaboration avec les instances étrangères, notamment européennes, permettrait d'augmenter le pouvoir d'action sur les très grandes structures. **En troisième lieu**, étant donné les risques de manipulations précités, il importe de s'assurer du respect de la liberté d'attention des usagers. **En quatrième lieu**, un devoir de diligence devrait être modulé en fonction des risques et de la capacité d'action des plateformes. **En cinquième lieu**, justement, une évaluation et une gestion des risques sont requises, ces derniers devant être 1) identifiés; 2) encadrés; 3) évalués; 4) validés; 5) mis à jour. Cette démarche de la plateforme est ensuite analysée par un organisme de contrôle et donne ensuite lieu à une publication pour informer le public. **En sixième lieu**, un régime spécifique peut être envisagé dans le cas de certaines applications de l'intelligence artificielle.

2.3 LCCJTI + identité

Mise en contexte. Si l'identité peut être multiple (personnelle, sociale, etc.), elle est généralement associée à l'unicité d'une entité. Elle donne lieu à un double mécanisme d'identification (opération de demande d'accès pour communiquer l'identité réclamée) et d'authentification (processus de contrôle vérifiant et validant ladite identité). Elle donne lieu à un traitement spécifique dans la LCCJTI (art. 40 à 62), d'abord sur les questions de biométrie et ensuite sur la certification numérique.

2.3.1 Tendances

Mise à jour des approches initiales. Au regard de l'analyse des textes effectuée, trois grandes tendances sont perceptibles. La **première** est que l'époque où les infrastructures à clés publiques étaient les seules solutions applicables est révolue. Si cette technologie a été très largement régulée par les lois tant américaines (et notamment le *Utah Digital Signature Act* dès 1995; Loi fédérale de 2001) qu'européennes (Directive de 1999 mais aussi eIDAS en 2014), une tendance vers plus d'ouverture semble requise. La LCCJTI n'a pas divergé de cette tendance initiale et a adopté des dispositions en ce sens (art. 47 à 62). Des dispositions qui n'ont donné lieu à aucun traitement jurisprudentiel, notamment à cause du fait que l'utilisation de cette technologie n'est nullement obligatoire. Aussi, plus de 20 ans plus tard, on peut se demander, d'une part, s'il faut élargir dans la LCCJTI les moyens de s'identifier (comme en Corée en 2023) et, d'autre part, si l'on doit légiférer sur la signature (comme en Europe), ce que le législateur québécois a refusé de faire en 2001.

Approche relative aux données biométriques. L'approche choisie en matière de biométrie était en revanche assez isolée, peu de juridictions ayant fait le choix d'établir un régime propre à ce type de données. À ce jour, on peut constater le cas de l'Illinois (2008) et surtout de l'Europe avec le RGPD (2016) où une référence au consentement explicite semble de mise. Cette tendance récente semble en accord avec la position choisie en 2001 par la LCCJTI, bien que l'article 43 LCCJTI soit d'une plus grande rigueur que l'approche européenne. En revanche, il faut mentionner que la proposition européenne de mettre à jour le règlement eIDAS ne traite pas de biométrie, laissant le soin au RGPD de régir ces questions.

Adoption agnostique. La **seconde** tendance qui semble s'apercevoir est qu'il est sans doute judicieux de maintenir une approche législative plutôt neutre sur le plan technologique. Bien que présente en 2001, un certain renforcement de ce principe semble de mise aujourd'hui. On peut l'apercevoir dans la récente loi coréenne (2023); on peut aussi le constater par l'infrastructure mise en place par le gouvernement américain (2022) où le concept d'authentification multi-facteur est valorisé, quelle que soit la technologie employée. C'est aussi vrai auprès du Gouvernement du Canada (2023) et certains services gouvernementaux du Québec. Cela dit, ces avancements ne requièrent aucun changement de la LCCJTI.

Vers une identité « régalienne ». Une **troisième** tendance observable est, d'une part, le besoin d'une identité capable d'interagir avec les organismes étatiques et, d'autre part, de favoriser les différents fournisseurs d'identité. Relativement au premier point, on sent le besoin de mettre en place un « triangle de confiance » pour que l'utilisateur puisse s'identifier dans des hypothèses en lien avec les services de l'État. À ce sujet, la référence à des normes techniques semble de mise.

Même aux États-Unis, naturellement moins enclins à des « formules imposées », un projet de loi est à l'étude afin de permettre à des agences gouvernementales de servir de source autorisée pour valider les attributs des citoyens américains. Après, cette tendance présente néanmoins certaines failles et des différences de culture prévalent notamment entre l'Europe et l'Amérique. Aux États-Unis, par exemple, tout comme en Corée, on envisage des partenariats public / privé, à la différence du Yukon dont le modèle est public. En Europe, la mise à jour du règlement eIDAS vise à abandonner les seules solutions d'identité numérique pour plutôt promouvoir la fourniture d'attestations électroniques d'attributs d'identité.

Chaînes de blocs. Comme mentionné, les tendances en matière d'identité sont plutôt agnostiques. Or, un sujet à la mode est de généraliser les structures décentralisées telles que les chaînes de blocs qui permettraient notamment aux utilisateurs de gérer eux-mêmes les attributs les concernant. Cette mode est contraire à l'approche « régalienne » précitée. Peu identifiée dans les lois étudiées, nous y trouvons néanmoins référence dans une loi coréenne. Avec égard, et au regard de la comparaison effectuée, nous croyons qu'il faut agir avec prudence dans l'utilisation d'un pareil procédé.

Hypertrucage. Notons pour finir sur ce point que la problématique déjà évoquée de l'hypertrucage est susceptible d'avoir un effet important sur l'identité des personnes. Nous n'avons néanmoins pas trouvé de textes de loi traitant spécifiquement de cet état de fait, du moins dans le contexte d'identité (une loi chinoise évoque l'hypertrucage mais pas spécifiquement concernant l'identité).

2.3.2 Propositions

Si les dispositions sur la biométrie sont intéressantes, notamment en donnant un certain pouvoir de contrôle à la *Commission d'accès à l'information* (CAI), elles ne devraient pas se trouver dans la LCCJTI. En effet, il serait sans doute plus judicieux de les intégrer dans les deux lois relatives à la protection des renseignements personnels dont elles relèvent davantage. Après, quant à la mise à jour de ces règles, nous avons notamment considéré la rigueur de l'article 43 qui, en matière de traçage de personnes, notamment en droit du travail, est sans doute plus rigoureuse que le RGPD. Également, il faut étayer les dispositions sur l'identité qui pour le moment ne considèrent que la seule situation des infrastructures à clés publiques. Au-delà de cette technologie qui était quasiment la seule en 2001, il importe de favoriser l'utilisation de technologies agnostiques telles qu'aperçues dans plusieurs législations. Enfin, la migration vers un nouveau système d'identité numérique devrait faire l'objet d'analyse d'incidences afin d'évaluer les risques associés à ces changements.

2.4 LCCJTI + sécurité

Mise en contexte. En 2001, la LCCJTI orchestrait les enjeux de la sécurité autour des trois piliers habituels en la matière, à savoir, la disponibilité, l'intégrité et la confidentialité. Concernant la **première**, la disponibilité, est souvent l'« enfant pauvre » de cette triade en matière de sécurité, trop d'accent sur elle allant à l'encontre de la confidentialité. La **deuxième**, l'intégrité, est en revanche grandement évoquée dans la LCCJTI et notamment à l'article 6. Elle constitue la pierre angulaire de cette loi, et ce, durant tout le cycle de vie du document. Enfin, la **troisième** notion, soit la confidentialité, demeure l'élément le plus communément associé à la sécurité. Il est principalement identifié à l'article 25 qui associe expressément confidentialité et sécurité.

2.4.1 État des tendances

Inflation. D'abord, le premier constat est de faire face à une relative inflation des textes en matière de cybersécurité, ce qui n'était évidemment pas le cas en 2001. En fait, un morcellement des règles de sécurité se constate selon que l'on utilise une approche par discipline (droit de la consommation, du travail, bancaire, etc.), fonctionnelle (anonymisation, profilage, etc.) ou technologique (intelligence artificielle, chaînes de blocs, etc.). Cette approche par silo est possiblement problématique et il serait sans doute plus pertinent d'apporter une approche globale axée sur les risques encourus. Aussi, la référence aux normes techniques pour un sujet comme celui-ci semble particulièrement incontournable.

Lutter contre les silos. Le constat premier est que la sécurité est souvent tributaire de thématiques, dépendant de textes propres à un type de données (ex. : données ouvertes) ou d'infrastructure (ex. : sécurité de l'infonuagique) plutôt qu'une vision holistique. Le meilleur exemple est le droit américain où aucune loi transversale existe, privilégiant plutôt des textes pour la santé, le domaine bancaire, la vie privée des enfants, etc., et selon l'activité réglementaire des différentes instances fédérales (*Securities Exchange Commission*, *Federal Trade Commission*, etc.) ou étatiques. Au Canada, on constate ce même phénomène dans le domaine financier ou au regard des renseignements personnels des consommateurs (C-27). D'ailleurs, une protection de la sécurité qui s'analyse au regard de la protection des renseignements personnels est en soi « thématique » et de ce fait peut être vue comme étant problématique, notamment parce qu'elle n'encadre pas les données autrement confidentielles telles que des secrets commerciaux. Au-delà de la sécurité de renseignements non personnels, on constate aussi une série de lois à travers le monde qui concerne spécifiquement les données relatives aux infrastructures. Il serait en revanche pertinent de déterminer si un tel sujet relève davantage de la LCCJTI ou de la *Loi sur la cybersécurité et du numérique*.

Tendance d'une approche fonctionnelle. Cette approche se constate à deux niveaux : d'une part, au niveau « macro », toute une série de lois visent à encadrer un risque spécifique tel que, par exemple, la cyberintrusion. Ce n'est donc pas l'objet qui est visé, mais une menace en particulier. D'autre part, on constate des textes qui encadrent un mécanisme à mettre en place (ex. : comme l'anonymisation des données).

Tendance de cadres techno-centrées. Enfin, on constate une tendance malheureuse selon laquelle les lois et autres textes ciblent une technologie en particulier. Par exemple, aux États-Unis, on aperçoit des directives de la Maison blanche concernant l'Internet des objets, l'infonuagique, et bien entendu l'intelligence artificielle. L'Europe suit une même tendance avec les articles 10 et 15 de la *Législation sur l'intelligence artificielle* de juin 2023. Cela dit, ce texte récent présente l'avantage de faire référence à l'article 42 à un autre Règlement de 2019 relatif aux modalités de certification. Notons enfin que cette approche sectorielle n'est pas le propre des lois et se retrouve aussi au niveau des normes techniques. Ainsi, par exemple, il existe une norme générale sur la sécurité de l'information (ISO 27002) et une autre, guère différente, sur les données hébergées dans des espaces infonuagiques (ISO 27018).

Analyse de risques. Si nous sommes parfois critiques sur l'approche par silo précédemment décrite, nous croyons important de relever une autre tendance selon laquelle une valorisation généralisée est faite vis-à-vis des analyses de risques. Celle-ci se trouve notamment dans le règlement européen

sur l'intelligence artificielle, l'ACEUM (section 19.15). Une approche qui se retrouve aussi dans la Loi 25 sur la protection des renseignements personnels.

Délégation normative. Enfin, l'un des derniers constats que l'on puisse faire concerne la délégation presque systématique des lois vers des organismes normatifs. Elle se vérifie dans de nombreux textes tels que par exemple le *Règlement européen sur l'intelligence artificielle* (considérant 61) ou la *Directive 2022 / 2555 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité* (article 25). Si cette approche semble incontournable du fait de la souplesse que cette manière de faire autorise, il faut néanmoins avoir à l'esprit des risques en termes de légitimité de recourir trop facilement à des règles de « droit mou ».

2.4.2 Propositions

Tel que mentionné, nous croyons important de rappeler qu'il nous appert ne pas être opportun de développer des règles qui soient trop spécialisées et trop associées à une technologie ou un secteur donné. Il importe donc de valoriser une approche globale de la sécurité. Également, si la référence aux normes techniques est sans doute nécessaire, il faut avoir conscience des travers qu'un recours trop systématique à ces règles peut avoir. À cet égard, le Comité d'harmonisation a sans doute un rôle à jouer tant dans l'identification des normes que dans la validation de celles-ci.

Nous croyons aussi que les articles 25 et 26 de la LCCJTI mériteraient une réécriture afin d'une part de clarifier leur portée et de mieux présenter la triade précitée (disponibilité – intégrité – confidentialité) qui devrait se retrouver dans les deux dispositions.

INTRODUCTION

Ce rapport porte sur l'avenir qu'il est possible de donner à la *Loi concernant le cadre juridique des technologies de l'information*[2] (ci-après « LCCJTI »). Il expose les tendances qui doivent être considérées afin d'identifier les mises à niveau nécessitées par les évolutions des deux dernières décennies.

Depuis 2001, l'importance des technologies dans la vie des personnes a continué de croître au point de modifier substantiellement et durablement plusieurs façons de faire. Cela justifie d'évaluer les dispositions de la LCCJTI qui doivent être modifiées, maintenues ou autrement considérées et nous avons aussi examiné l'opportunité d'insérer des dispositions afin de refléter les développements qui ne pouvaient être prévus en 2001.

La LCCJTI porte sur un univers transversal embrassant un vaste éventail d'activités et de situations. L'univers des technologies de l'information est sujet à des changements accélérés et comporte des enjeux relevant aussi bien de la sécurité juridique ou technique que des droits fondamentaux.

Les enjeux associés aux technologies de l'information se manifestent généralement sous la forme de risques perçus ou supposés.

Le droit est appelé à fournir les cadres afin de mieux appréhender et gérer les risques inhérents à des phénomènes technologiques qui découlent à la fois des possibilités des objets techniques que des comportements de celles et ceux qui en ont la maîtrise.

La LCCJTI procure un encadrement des dispositifs technologiques fondamentaux associés aux technologies de l'information. Partie intégrante du droit commun québécois, elle se caractérise par une appréhension originale des réalités technologiques. Formulée autour de la notion de technologie, la LCCJTI s'attache à énoncer les règles de droit relativement à l'accomplissement de fonctions assurées au moyen des technologies. À cette fin, elle retient un sens inclusif des technologies et une approche permettant dans toute la mesure du possible d'accueillir les dispositifs nouveaux qui ne manquent pas d'émerger.

Compte tenu de cette nécessaire ouverture vers l'innovation, la LCCJTI postule que les normes qui encadrent l'usage des technologies émanent d'une pluralité d'univers normatifs. La trame du présent rapport reflète ces caractéristiques fondamentales de la LCCJTI et de son contexte d'application.

Comme toute loi, mais singulièrement lorsqu'il s'agit d'une loi vouée à encadrer des réalités aussi volatiles que les technologies de l'information, la LCCJTI doit se lire et s'interpréter dans des contextes diversifiés et en constante évolution. À cet égard, il faut envisager cet exercice de réflexion sur les perspectives de mise à jour de cette loi sur les technologies comme un instantané reflétant les tendances et les constats observables aujourd'hui.

Dans la première partie, nous identifions les tendances observables au niveau des situations de faits caractérisant l'univers des technologies de l'information. Cela permet une mise en perspective avec

---

[2] RLRQ c. C-1.1.

les tendances qui prévalaient en 2001. Nous identifions également les tendances relatives à l'état du droit afin de brosser un portrait de caractéristiques des lois et autres règles de droit qui encadrent les activités visées par les législations relatives aux technologies de l'information.

Dans la seconde partie, quatre domaines de droit traités dans la LCCJTI et susceptibles d'être altérés par la réalité de 2023 sont passés en revue. C'est ainsi que sont examinés les tendances à l'égard de la formulation et de l'application des normativités des univers marqués par les technologies de l'information. De même, il est fait état des tendances des lois organisant les responsabilités de ceux qui interviennent dans la mise à disposition et la transmission des informations. Les tendances et enjeux associés à l'identité entendue comme l'ensemble des attributs associés à une personne permettant de la relier à d'autres données sont examinés. De même, sont passées en revue les tendances des efforts législatifs en matière de sécurité de l'information.

Tout au long des développements, des propositions afin d'ajuster la voilure de la LCCJTI sont présentées. Étant donné le caractère transversal de la démarche, certaines propositions demeurent générales et doivent être envisagées comme des invitations à investiguer plus à fond les éventuels tenants et aboutissants des mesures spécifiques qui pourraient être adoptées et mises en œuvre.

PARTIE 1 – LCCJTI+ : TENDANCES GÉNÉRALES EN DROIT DU NUMÉRIQUE

1.1 Tendances et état des faits

Impératif de cohérence. L'une des principales finalités de la LCCJTI est d'assurer la cohérence du droit québécois avec les situations caractéristiques d'un monde de plus en plus marqué par le recours aux technologies de l'information pour accomplir différents actes juridiques. Depuis 2001, l'importance des technologies dans la vie des personnes a continué de croître. On passe ici en revue les principales tendances qui continuent de persister et qui doivent être prises en considération lorsque l'on évalue les mises à niveau qu'il conviendrait d'apporter à la législation.

1.1.1 Tendances et risques

Métamorphoses du numérique. Le numérique change les conditions de vie et modifie les façons de faire. Il rend obsolètes certains modes de fonctionnement et en fait émerger d'autres. Les lois doivent accompagner les transformations induites par les évolutions technologiques. Les mutations induites par le numérique requièrent une capacité accrue des États d'évaluer les changements dans les façons de faire et leurs incidences sur les cadres juridiques. Il faut assurer les mises à niveau des règles.

Normes juridiques et normes issues des configurations. Dans les univers issus de l'usage des technologies de l'information, les droits et les obligations découlent aussi bien des normes par défaut intégrées dans les objets technologiques que par les lois. Nous sommes en présence d'une normativité résultant principalement de décisions de gestion des risques prises par les régulateurs et les autres acteurs. Par leurs décisions et leurs comportements, l'ensemble des producteurs de normativités créent et relaient à leurs cocontractants et partenaires les risques engendrés par la normativité qui leur est applicable.

Souveraineté et cyberespace. Les États et les autres producteurs de normes ne peuvent prétendre à l'entière souveraineté dans le cyberespace, mais ils conservent une pleine capacité de formuler des règles qui engendrent des risques pour les acteurs. C'est dans un tel contexte qu'il convient de situer les tendances pertinentes à la mise à niveau d'une loi visant à procurer un cadre juridique pour les situations dans lesquelles les technologies de l'information tiennent une place significative. Évidemment, les risques de 2023 sont sensiblement différents de ce qui pouvaient être identifiés en 2001, du fait de raffinement associé à de nouveaux outils.

Observer. Comme le signalait Jeanne Proulx[3], pour apprécier les changements qui doivent être apportés aux cadres législatifs, il importe d'observer ce qui change et ce qui ne change pas. Au nombre des changements, il est clair que l'information circule plus que jamais dans une pluralité de canaux et que ces communications peuvent être captées et conservées dans des documents dont les supports peuvent faire appel à diverses technologies. Quel qu'en soit le support, le document répond aux besoins de consigner l'information afin de la communiquer, de la consulter de la transmettre et de la conserver. Ce qui continue de changer toutefois, ce sont les supports qui sont

[3] Jeanne PROULX, « Méthodologie d'intégration des technologies de l'information dans le droit : l'exemple du Québec », dans Georges Chatillon, *Droit de l'administration électronique*, Bruxelles, Bruylant, 2011, 363-372.

en continuel renouvellement. Tout au long de l'histoire humaine, l'information a été transférée d'un support à l'autre, en faisant appel à des technologies différentes. En somme, les technologies changent, les façons de faire se modifient, mais les impératifs qui doivent être assurés par le droit demeurent. Jeanne Proulx énumérait certaines des préoccupations les plus importantes auxquelles le droit a mandat de répondre :

- la protection des valeurs fondamentales […];
- la liberté de choisir le support et les technologies en fonction des besoins de communiquer et de consigner l'information;
- la protection de la vie privée et de la confidentialité;
- la protection des usagers des technologies de l'information et des consommateurs;
- la recherche de la sécurité, notamment des transactions;
- le besoin de constance (de prévisibilité) du droit.

Respect des valeurs. Pour assurer le respect de ces impératifs, il faut un cadre juridique stable assurant le respect des valeurs et qui ne changera pas à chaque fois qu'un nouvel objet technique apparaît. Cette constance et cette prévisibilité sont des conditions importantes d'un cadre juridique efficace et en mesure de procurer les encadrements et les équilibres nécessaires dans un monde en changement accéléré.

1.1.1.1 Mutation des risques

Risques accrus et diversifiés. Au début du siècle, on tendait à percevoir les risques du numérique en fonction de la reconnaissance par le droit des transactions réalisées par les moyens technologiques. Deux décennies plus tard, nous voilà en présence d'un espace d'interactions ayant vocation à embrasser la presque totalité des dimensions de la vie sociale. De ce fait, les risques se trouvent augmentés et sont plus diversifiés. Puisque pratiquement tous les champs d'activité sont affectés par les mutations associées à la généralisation du recours aux technologies de l'information, on observe un décloisonnement des risques. Ceux-ci sont ressentis sans égard aux frontières géographiques et affectent les individus aussi bien dans leur vie professionnelle que dans leur vie personnelle. Les frontières entre l'une et l'autre tendent d'ailleurs à se dissoudre. Les libertés fondamentales, de même que les autres droits des personnes, peuvent ainsi se trouver à risque.

1.1.1.1.1 Les risques transcendent les frontières

Comportements et configurations. Dans les univers connectés, les risques émanent de partout. Ils peuvent provenir des comportements d'acteurs situés très loin des frontières territoriales d'un État. Ils émanent aussi des configurations techniques. La régulation découle donc de ces configurations techniques qui, par défaut, influent sur les droits et les obligations. Elle résulte souvent aussi bien du droit national du pays où l'on se trouve que du droit des ordres juridiques des entités en position d'exercer une influence sur les autres lieux d'élaboration de normes.

Coordination et équilibrage. Certains lieux de normativité produisent des normes ou des processus de coordination, tandis que d'autres fonctionnent comme des espaces de négociation ou d'équilibrage appliquant des régulations dans un rapport de dialogue avec d'autres lieux de

normativité. Par exemple, c'est souvent à la suite d'invitations de la part des organisations internationales que les États sont amenés à relayer des normes dans leurs législations. Citons ici la *Convention sur la cybercriminalité*[4], laquelle a été mise de l'avant par les instances européennes et ouverte à la signature d'autres pays. Les objets peuvent être configurés de manière à accroître les risques de certains et minimiser les risques supportés par d'autres.

Risque de non-conformité. Compte tenu de cette insensibilité aux frontières, il importe d'envisager les risques de possible non-conformité à une gamme étendue de normes. Si les lois du territoire sur lequel on se trouve s'imposent d'office, on peut aussi avoir à composer avec des règles, légales, techniques ou des pratiques qui émanent d'un vaste ensemble de lieux normatifs.

1.1.1.1.2 Les risques concernent des acteurs professionnels ou non

Distinctions brouillées. Les espaces d'interactions rendus possibles par les technologies peuvent mettre en présence aussi bien des professionnels que des individus consommateurs. En cela, la distinction autrefois plus nette entre commerçant et consommateur tend à s'estomper. Depuis 2001, la place tenue par les intermédiaires s'est considérablement accrue. Prenant appui sur de tels environnements, se sont développés une kyrielle d'espaces dotés de puissantes capacités de mettre en présence des offreurs et des demandeurs de services ou d'information. Ces « lieux », qui n'étaient à une certaine époque que des blogues, sont devenus des espaces virtuels capables de mettre en présence des offreurs de biens et de services et des personnes désireuses d'y accéder. Cela a permis l'émergence de nombreuses plateformes dans lesquelles peuvent se dérouler des conversations, des diffusions de sons, textes ou images. Aussi, ces espaces sont devenus d'importants lieux dans lesquels se déroulent diverses relations contractuelles. Un développement aussi fulgurant a porté l'autrice Julie Cohen à considérer les plateformes en ligne comme étant « the core organizational form of the emerging information economy »[5].

Économie collaborative. En 2018, le *Rapport du Groupe de travail sur l'économie collaborative*[6] observait que les plateformes et applications fonctionnant grâce aux technologies numériques « facilitent et multiplient les transactions entre particuliers et organisations offrant des biens, des services ou des ressources telles que la connaissance et les idées ». Les auteurs constataient que « les plateformes numériques opèrent un changement d'échelle en rendant disponible n'importe quel actif et en mettant en relation, instantanément et simultanément ou de façon planifiée, des particuliers et des organisations ». C'est ainsi que dans de multiples secteurs d'activité sont apparus des écosystèmes reposant sur la satisfaction de besoins, notamment en facilitant l'accès d'un ensemble d'individus qui ne sont pas nécessairement des professionnels des activités concernées. Surtout, la substitution de plateformes numériques aux intermédiaires de l'économie traditionnelle a permis de mettre directement en relation des particuliers, des entreprises et des organisations notamment vouées aux échanges entre pairs.

---

4 Conseil de l'Europe, *Convention sur la cybercriminalité*, Budapest, 23 novembre 2001, en ligne : <http://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/185>.

5 Julie COHEN, « Law for the Platform Economy », (2017) 51 *University of California Davis Law Review*, 135.

6 Rapport du Groupe de travail sur l'économie collaborative, Gouvernement du Québec, 2018, p. 81, en ligne : <https://www.economie.gouv.qc.ca/bibliotheques/economie-collaborative/groupe-de-travail-sur-leconomie-collaborative>.

Mutations. Il en est résulté d'importantes mutations dans les pratiques ayant cours dans divers secteurs d'activité. Les repères culturels et économiques ayant motivé les cadres réglementaires des activités se sont trouvés remis en question. Par-dessus tout, se pose toutefois la question de la répartition des responsabilités entre les offreurs, les demandeurs, les consommateurs, les autorités publiques et les plateformes (voir la section 2.2). Désormais, plusieurs secteurs d'activité sont concernés par la disponibilité d'espaces en ligne possédant un fort potentiel d'habiliter divers acteurs à diffuser des idées ou des offres de produits ou de services. Comme on a pu l'observer dans le domaine du transport par taxi ou de la location à court terme de logements, cela amène à s'interroger sur les responsabilités devant incomber à ces acteurs intermédiaires que sont devenus les plateformes en ligne régies par l'article 22 de la LCCJTI.

1.1.1.1.3 Les risques concernant la sécurité et les libertés fondamentales

Sécurité et libertés. Les mutations dans les conditions des échanges d'information ne peuvent manquer d'avoir des effets sur la façon d'envisager le droit et les droits. Le droit appréhende les réalités à travers des catégories et des qualifications. Le développement de technologies de l'information engendre des transformations qui remettent en cause les catégories par lesquelles on avait l'habitude de définir les cadres juridiques. La numérisation et la généralisation des réseaux paraissent exercer une influence de mutation et une influence d'amplification de tendances. On peut parler d'une influence de mutation lorsque les changements induisent une rupture dans les logiques, les façons de faire et les perceptions. On parlera d'une influence d'amplification lorsqu'il n'y a pas de changement radical dans les logiques et les façons de faire, mais une modification dans la perception des risques ou des enjeux. Ces deux types d'influence contribuent aux mutations que l'on commence à observer dans les façons d'envisager les droits fondamentaux.

1.1.1.2 Augmentation des risques

Risques accrus. La généralisation de la possibilité d'accomplir pratiquement toutes les activités dans les univers construits par les technologies a forcément eu pour conséquence d'accroître les risques qui doivent être considérés. Les risques sont présents dans l'ensemble des secteurs d'activité. Ils se manifestent en prenant souvent en défaut les cadres juridiques conçus pour s'appliquer à des activités situées dans les espaces physiques. Par exemple, la capacité de réaliser en ligne des transactions afin de louer des logements à court terme est venue compliquer l'application des règles régissant les bâtiments locatifs.

Application des lois. Dans plusieurs milieux, on se résigne à tenir pour acquis qu'il est impossible pour les États d'assurer l'application de leurs lois à l'égard des objets technologiques. Ainsi, on déplore que les interdits de publier prévus par les lois, afin notamment de protéger les enfants et les victimes de crimes, sont régulièrement ignorés par des gens qui diffusent sur les réseaux sociaux des renseignements qu'il est interdit de diffuser en vertu des lois. Des voix de plus en plus nombreuses s'élèvent pour rappeler qu'on ne pourra longtemps tolérer que les lois qui interdisent quelque chose sur la terre ferme cessent magiquement de trouver application lorsqu'on est sur Internet ou lorsqu'un objet technique nouveau vient tout déjouer. Par exemple, à quoi bon conserver des lois qui interdisent aux médias traditionnels d'identifier un enfant victime de crime si on ne trouve pas le moyen d'appliquer ces règles dans les espaces d'Internet ? Il y a là un enjeu de légitimité même des lois. Maintenir des lois qui réservent un régime de deux poids deux mesures

selon que l'activité est en ligne ou sur la terre ferme contribue à miner la légitimité même du droit étatique.

1.1.1.3 Diversification des risques

Risques gérés par les individus. Selon les modèles dominants, ce sont les individus utilisateurs qui sont *a priori* appelés à reconnaître et gérer les risques auxquels ils sont exposés. Une telle approche, héritée des idées fondatrices d'Internet, postule que l'individu serait en mesure de connaître et d'évaluer les risques qui le confrontent et de prendre ses décisions en conséquence. Par exemple, la mise en place de régulations efficaces est entravée par la persistance à considérer les données que chacun d'entre nous produit uniquement comme une ressource que les individus doivent protéger en consentant à leur usage. Pourtant, une part croissante des risques auxquels sont exposés les populations sur Internet ne peuvent être appréhendés comme une affaire relevant des seuls individus. La capacité de reconnaître et d'apprécier les risques requiert souvent des expertises qui ne peuvent être possédées par les usagers agissant à titre individuel. Cela appelle à la nécessité de mobiliser des instances publiques de même que les ressources associatives afin de disposer de moyens conséquents pour gérer les risques.

1.1.1.3.1 Les objets

Objets traitant de l'information. Dans le monde connecté, les objets ne sont plus seulement des outils qu'on utilise pour accomplir des tâches. Ils sont dotés d'importantes capacités de traiter de l'information. De ce fait, ces objets produisent des réglementations qui, par défaut, s'imposent à nous. Par exemple, les automobiles désormais proposées sur le marché comportent des capacités considérables de collecte, de traitement et d'analyse d'information.

1.1.1.3.2 La viralité

Risque inhérent. La viralité est de plus en plus perçue comme un risque inhérent aux environnements techniques fonctionnant en réseaux. Dans les espaces en réseaux, les informations se diffusent par défaut comme des virus. Les mots, les images peuvent être mis en ligne par toute personne possédant un appareil connecté. Ils se trouvent généralement disponibles et peuvent être reçus par des usagers qui à leur tour se trouvent en mesure de les partager à d'autres qui peuvent à leur tour les repartager. Une telle viralité peut se répéter à l'infini. La viralité accentue les risques associés aux contenus ou aux activités préjudiciables.

1.1.1.3.3 Les capacités de reproduction à l'identique

Capacités banalisées. La tendance lourde déjà présente depuis plusieurs décennies, à voir se banaliser la faculté de réaliser des copies difficiles à distinguer de l'original, a conduit les législateurs à revoir les notions d'original et de copie. Avec les technologies facilitant l'*hypertrucage* (*deepfake*), un procédé de manipulation ayant recourt aux algorithmes d'apprentissage profond (*deep learning*) pour créer des trucages ultraréalistes, c'est la différenciation entre le réel et la fiction qui pose un défi colossal. Cela interpelle le cadre juridique régissant le statut de la copie et de l'original.

1.1.1.3.4 Le rôle crucial des algorithmes

Objets techniques qui régulent. Une part grandissante des activités dans le monde connecté est supervisée au moyen de procédés faisant usage d'algorithmes. À bien des égards, les algorithmes régissent nos comportements autant, sinon plus que le font les lois et règlements régissant nos activités quotidiennes. Les algorithmes sont au cœur des activités qui se déroulent dans les environnements en ligne. Il devient essentiel de mettre en place un régime d'imputabilité et de responsabilité pour le fonctionnement de ces dispositifs. Les algorithmes sont des objets techniques particuliers : en régulant les informations et les objets, ils régulent les comportements. En y ayant recours, on peut rendre possibles ou impossibles des activités. On peut fixer les prix selon différents paramètres, montrer ou cacher des messages. Les algorithmes font des calculs en temps réel pour déterminer quel message publicitaire sera affiché sur une page Web, quels biens de consommation seront proposés à l'internaute, quelles émissions seront suggérées à l'abonné d'une plateforme. Réguler les processus fondés sur des algorithmes, c'est obliger ceux qui les utilisent à garantir qu'ils fonctionnent en conformité avec les principes des lois étatiques et les droits fondamentaux. Cela suppose une capacité de vérification transparente.

1.1.1.3.5 Les enjeux de souveraineté et d'interrégulation

Souveraineté et réseaux. Dans un rapport paru à l'automne 2018, la Commission de réflexion sur la recherche en sciences et technologies du numérique[7], issue de plusieurs institutions de recherche françaises, constate que les conditions de la souveraineté nationale, fondée sur la maîtrise du territoire physique, sont radicalement modifiées. Le fonctionnement des réseaux complique la capacité effective des États de contrôler ce qui se passe sur leur territoire. On remarque que les conditions induites par la prééminence des environnements en réseaux forcent à s'interroger sur « […] les souverainetés numériques des États, des organisations ou des citoyens, […] ou des souverainetés supranationales ». La souveraineté doit désormais s'exercer dans des espaces de plus en plus virtuels. Il importe que les États se dotent des moyens de faire prévaloir les choix et les règles cohérents avec leurs valeurs. Ils doivent à la fois agir seuls et innover en se donnant les moyens d'agir en concertation avec les autres États.

Interrégulation. Prenant acte du fait qu'Internet est essentiellement construit sur un réseau technique ayant engendré un espace numérique au sein duquel se manifestent une pluralité de régulations, des auteurs réunis par Marie-Anne Frison Roche n'hésitent pas à analyser Internet comme un espace d'interrégulation[8]. Il existe un large consensus pour convenir qu'une pluralité de normes, de normativités sont appliquées dans l'espace-réseau. Mais quels sont les facteurs qui contribuent à déterminer, dans un contexte spécifique donné, laquelle des règles sera effectivement appliquée ?

1.1.1.3.6 Les capacités considérables de l'IA

Capacités considérables de traitement. L'intelligence artificielle (IA) désigne notamment ces capacités de traiter des masses gigantesques de données et d'information, de calculer des

---

7 Commission de réflexion sur l'éthique de la recherche en sciences et technologies du numérique d'Allistene, *La souveraineté à l'ère du numérique*, octobre 2018, en ligne : < https://www.allistene.fr/cerna/ >.

8 Marie-Anne FRISON ROCHE (dir.), *Internet, espace d'interrégulation*, Paris, Dalloz, 2016.

corrélations, de prédire, d'apprendre et d'adapter de façon automatisée des réponses aux situations changeantes. Cela permet des avancées majeures qui doivent bénéficier à tous. Mais l'IA vient avec son cortège de risques et de défis. C'est pourquoi il importe d'intégrer dans les lois les principes directeurs mis de l'avant pour encadrer le développement de ce type d'innovations. Il faut délimiter les droits et obligations des acteurs concernés par les processus ou les objets carburant à l'IA.

Déclaration de Montréal. La *Déclaration de Montréal pour un développement responsable de l'intelligence artificielle*[9] affirme que le développement et l'usage des systèmes d'IA doivent permettre d'accroître le bien-être de tous les êtres sensibles. Son utilisation doit se faire dans le respect de l'autonomie des personnes et celui de la vie privée. Les procédés fondés sur l'IA doivent aussi être compatibles avec les liens de solidarité entre les personnes et les générations. Ces systèmes doivent être soumis à l'examen et aux contrôles démocratiques. Ils doivent être compatibles avec la diversité sociale et culturelle. Leurs conséquences doivent être anticipées en fonction d'un principe de prudence. Le recours à de tels outils ne saurait avoir pour conséquence de déresponsabiliser les personnes qui en font usage.

Objets et leurs normes. Les objets comme les véhicules autonomes, les jouets « intelligents » ou les médicaments connectés intégrant des technologies d'IA comportent forcément des normes par défaut. Les objets techniques ne sont pas neutres : ils permettent, autorisent ou interdisent[10]. Les configurations par défaut des objets techniques comportent des régulations souvent mises en place dans le seul souci de répondre au « marché » sans égard aux exigences démocratiques. Ceux qui fabriquent des dispositifs, comme les véhicules autonomes, devront les configurer en reflétant les principes de la Déclaration.

Normes justifiées. Dans une société démocratique, les lois et les autres régulations, dont celles qui par défaut sont intégrées dans les objets intelligents, doivent reposer sur des justifications. Les valeurs exprimées dans la Déclaration de Montréal reflètent les consensus et justifient les exigences qui pourront être imposées par les lois aux usagers des objets et processus intégrant l'IA.

Principes à actualiser. L'actualisation de certains des principes de la Déclaration de Montréal va engendrer des remises en question des façons de faire. Par exemple, le principe de participation démocratique devra être concilié avec les revendications des entreprises à l'égard de leurs droits exclusifs sur les données qu'elles collectent et traitent via les procédés de l'IA. Il faudra aussi s'interroger sur la portée et les limites du principe d'équité et des exigences du consentement supposément libre et éclairé des individus et par lequel les grands joueurs industriels parviennent à accaparer la valeur des masses de données traitées par les procédés fondés sur l'IA. Des désaccords sont à prévoir sur l'ordre de préséance qui doit s'appliquer lorsqu'un principe de la Déclaration vient en conflit avec un autre. Est-ce que l'IA doit avant tout optimiser le bien-être de ceux qui sont déjà favorisés ou contribuer à mutualiser les risques de façon à protéger l'ensemble des membres de la collectivité ? Plusieurs des principes de la Déclaration vont se retrouver au cœur

---

9 *Déclaration de Montréal pour un développement responsable de l'intelligence artificielle*, (2017), en ligne : <https://declarationmontreal-iaresponsable.com/>.

10 Donald A. NORMAN, *Things That Make Us Smart*, Reading, Addison-Wesley, 1993, p. 243.

des argumentations que les divers groupes d'intérêts mettront de l'avant, afin de justifier des lois réglementant la configuration des objets « intelligents ».

1.1.2 Tendances et besoins

Processus en réseaux. Chercher à identifier tous les risques possibles, puis créer des règles pour les atténuer, est une tâche difficile et sans doute impossible. Cependant, les régulateurs peuvent travailler directement à réduire le temps de décalage entre le moment où un nouveau service ou produit provoque des dommages à un consommateur et le moment où le régulateur découvre le préjudice. La régulation en réseau découlant des processus multiples de gestion des risques constitue le principal vecteur de maintien des équilibres entre les risques et les précautions. Ces processus de régulation doivent fonctionner de façon à inciter l'ensemble des acteurs à minimiser les risques qui relèvent de situations sur lesquelles ils sont effectivement en mesure d'avoir une prise et à accroître le plus possible les risques des acteurs qui choisissent d'avoir des comportements dommageables ou qui augmentent indûment les risques des usagers légitimes.

1.1.2.1 Identification des besoins initiaux

Assurer le développement du numérique. Entrée en vigueur en novembre 2001, la LCCJTI répondait au besoin ressenti à l'époque d'assurer que les règles de droit ne constituent pas une entrave au développement des activités fondées sur l'utilisation des technologies de l'information. Il s'agissait, d'une part, de favoriser le commerce électronique. À titre d'exemple, on voulait définir largement certains termes afin que le droit ne soit pas un obstacle à la numérisation des rapports (citons notamment l'art. 5 LCCJTI). D'autre part, un objectif crucial de la LCCJTI était d'identifier certaines exigences en ce qui a trait à la sécurité documentaire. Par exemple, l'article 6 identifie les grandes lignes de ce que constitue l'intégrité d'un document. De façon assez innovante pour l'époque, la LCCJTI comportait également des dispositions pour assurer le respect de libertés fondamentales. On peut notamment penser aux articles 29 et 40 à 45 LCCJTI, dispositions qui parfois ne sont pas sans lien avec la protection des renseignements personnels.

1.1.2.2 Sophistication des besoins

Déstructuration des rapports sociaux. À l'heure actuelle, il apparaît que le numérique est susceptible de déstructurer en profondeur les rapports sociaux. Parmi les changements constatés, plusieurs sont susceptibles d'avoir une incidence importante sur des enjeux juridiques de premier plan :

Rapports de force à peaufiner : La généralisation des TI favorise les mutations des rapports de force entre les acteurs. Des acteurs, comme les fournisseurs d'espaces de dépôts de documents ou d'outils d'identification, sont en mesure d'infléchir les équilibres entre les participants aux transactions.

Opacité accentuée : L'effet combiné de la prééminence de solutions propriétaires dans le déroulement des interactions peut accentuer l'opacité.

Responsabilités reconsidérées : Les environnements technologiques redéfinissent les conditions d'exercice des responsabilités des acteurs immédiatement concernés par les transactions, mais aussi les tiers qui les rendent possibles.

Discriminations augmentées : Par défaut, le fonctionnement des outils techniques peut avoir des effets de discrimination. Par exemple, la prééminence de l'anglais dans les environnements numériques peut rendre difficile le fonctionnement en français.

Décisions automatisées : De même, les avancées de l'intelligence artificielle combinées à d'autres développements technologiques et sociaux ont accentué la tendance en faveur de l'automatisation des processus décisionnels. Cela sollicite des encadrements juridiques renforcés.

L'impératif de proactivité : Plutôt que seulement réagir aux crises engendrées par les « disruptions » numériques, les États doivent agir de façon proactive. Ils doivent se doter d'une meilleure capacité d'agir en réseau. Par exemple, le Québec[11] et la France[12] ont entrepris d'appliquer leurs lois fiscales aux acteurs d'Internet. Une telle approche doit être appuyée par une concertation qui renforcera l'efficacité des lois étatiques. Ce type de concertation qui existe déjà entre les États afin de lutter contre la cybercriminalité devra être étendu à d'autres secteurs du droit.

1.2 Tendances et état du droit

Tendances. Il est question dans cette section des tendances observables des législations et de l'état du droit dans les juridictions présentant des liens ou des similitudes avec le Québec.

1.2.1 Tendances et densification des approches juridiques

Du laisser-faire à l'encadrement plus dense. Alors que les encadrements juridiques mis en place au début du siècle semblaient motivés par un souci de laisser le plus possible de marge de manœuvre aux développeurs de l'économie numérique, on constate désormais un souci marqué d'intensifier les régulations applicables aux activités se déroulant en ligne.

1.2.1.1 Historique : du libertaire au libéral (1990–2010)

Anachronisme libertaire. Le droit du numérique bénéficie, depuis ses débuts, d'une incroyable tolérance de la part des cadres réglementaires. Alors que l'on aperçoit une augmentation des règles de responsabilité dans tous les domaines d'activité humaine, celui du numérique bénéficia, et bénéficie encore, d'un régime favorable aux acteurs commerciaux. La situation est notamment sensible au Québec et dans le reste de l'Amérique du Nord.

- c'est vrai pour les intermédiaires techniques[13];

---

11 *Loi sur la taxe de vente du Québec*, RLRQ c T-0.1, en ligne : <https://canlii.ca/t/6f3wd>, art 407 et ss. Voir aussi : Revenu Québec, Division de l'interprétation relative à l'imposition de taxes, Interprétation relative à la TVQ, application de l'article 411 dans un contexte de commerce électronique, ref. 19045892001, 18 décembre 2019, en ligne : <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.publicationsduquebec.gouv.qc.ca/fileadmin/produits_en_ligne/Fiscalite/pdf/19_045892_001.pdf >.

12 Loi n° 2019-759 du 24 juillet 2019 portant création d'une taxe sur les services numériques et modification de la trajectoire de baisse de l'impôt sur les sociétés (1), NOR : ECOE1902865L, ELI en ligne : <https://www.legifrance.gouv.fr/eli/loi/2019/7/24/ECOE1902865L/jo/texte; Alias : <https://www.legifrance.gouv.fr/eli/loi/2019/7/24/2019-759/jo/texte, JORF n°0171 du 25 juillet 2019.

13 Voir l'encart ci-dessous, page 19.

- c'est vrai en matière contractuelle où le cadre est minimaliste, même en matière de consommation[14];
- c'est vrai en matière de sécurité où le cadre quant aux mesures à suivre est très peu développé[15];
- c'est vrai en matière de normativité où l'intervention législative a été faible, laissant une place importance à l'autorégulation[16];
- c'est vrai en ce qui a trait au développement de nombreuses plateformes[17]; etc.

Construction libérale. À la fin des années 1990, notamment à la suite de motivations selon lesquelles il ne fallait pas entraver le développement de cette industrie naissante, mais aussi que la capacité de contrôle était moindre (ce qui a grandement changé désormais)[18], une série de lois favorables a été adoptée. Si la donne a changé dans certaines juridictions, notamment européennes, le très récent accord « Canada – États-Unis – Mexique » (ACEUM) valorise encore cette tendance exonérante

> (19.17) 1. Les Parties reconnaissent l'importance vitale de la promotion des services informatiques interactifs, y compris pour les petites et moyennes entreprises, pour la croissance du commerce numérique.
>
> [...]
>
> 3. Aucune Partie n'impose la responsabilité à un fournisseur ou à un utilisateur d'un service informatique interactif à l'égard, selon le cas :
>
> a) de toute mesure prise volontairement et de bonne foi par le fournisseur ou l'utilisateur pour restreindre l'accès ou la disponibilité de contenu qui est rendu accessible ou disponible au moyen de la fourniture ou de l'utilisation de ses services informatiques interactifs et que le fournisseur ou l'utilisateur considère comme nuisible ou inadmissible;

---

14 On peut penser au tout récent document consultatif de la part de la Commission du droit de l'Ontario (Law Commission of Ontario, LCO Consumer Protection in the Digital Marketplace Consultation Paper, juin 2023) qui milite pour un renforcement des droits du consommateur numérique.

15 *Infra*, Section 2.4.

16 *Infra*, Section 2.1.

17 Il est intéressant de voir comment la plateforme *Uber* a d'abord été autorisée par le biais d'une entente spéciale (Entente entre le ministre des Transports, de la mobilité durable et de l'électrification des transports et Uber Canada Inc., du 9 septembre 2016; Entente relative aux exigences de conformité fiscale au Québec, à l'égard des chauffeurs utilisant les plateformes « uberX », « uberXL » ou « uberSELECT », entre le ministère des Finances du Québec et Uber Canada Inc., du 15 août 2016) et ensuite a été légitimée par la modification de la loi applicable (*Loi concernant le transport rémunéré de personnes par automobile,* RLRQ c T-11.2, article 1.). Peu de choses aussi sur les plateformes liées à l'hébergement.

18 *Supra*, Section 1.1.

b) de toute mesure prise pour permettre ou rendre disponible les moyens techniques permettant à un fournisseur de contenu informatif ou à d'autres personnes de restreindre l'accès au contenu qu'il juge nuisible ou inadmissible.[19]

Tendance qui se retrouve dans la jurisprudence, au Québec par exemple[20] ainsi qu'au Canada[21].

Tableau 1
Responsabilité conditionnelle des intermédiaires techniques

	Année	Noms des lois	Irresponsabilité de principe	Article ou Section	Jurisprudence (exemples)	Commentaires
États-Unis	1998	DMCA[22]	Oui	Section 512	*Perfect 10, Inc*. v *CCBill LLC,* 488 F.3d 1102 (9th Cir. 2007). Viacom Int'l Inc. v. YouTube Inc., 940 F. Supp. 2d 110 (SDNY 2013) Twitter, Inc. v. Taamne 598 U.S. 471 (2023) Gonzalez v. Google LLC, 598 U.S. 617 (2023)	Modèle historique qui généralise le régime d'exonération de ce que l'on n'appelait pas encore les plateformes (intermédiaires techniques)
Canada	2012	LDA[23]	Oui	27 (2.3)	Société canadienne des auteurs, compositeurs et éditeurs de musique c. Assoc. canadienne des fournisseurs Internet, 2004 SCC 45 Crookes v. Newton, 2011 SCC 47 *Warman v. Fournier,* 2012 FC 803 *Google Inc*. v. *Society of Composer*s, 2017 SCC 34	Régime exonérant pour des règles adoptées en 2012 (c'est-à-dire très tard par rapport aux USA et UE)
Québec	2001	LCCJTI[24]	Oui	22 et 27	Prud'homme c. Rawdon (Municipalité de), 2010 QCCA 584 *A.B*. c. *Google*, 2023 QCCS 1167	Jurisprudence très rare. Tendance exonérante forte avec pour seule exception le récent jugement contre Google.

19 *Accord Canada–États-Unis–Mexique (ACEUM)*, chapitre 19, Commerce numérique, art. 19.17, en ligne : <https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cusma-aceum/text-texte/19.aspx?lang=fra>.

20 *Lehouillier-Dumas* c. *Facebook*, 2021 QCCS 3524 (para. 59 et ss.).

21 *Crookes* c. *Newton*, 2011 CSC 47, para. 16.

22 Voir notamment le *Digital Millenium Copyright Act* (17 U.S.C. § 512) ou le *Communications Decency Act* (47 U.S.C. § 230).

23 Voir notamment les amendements à la *Loi sur le droit d'auteur* de 2012.

24 Loi concernant le cadre juridique des technologies de l'information, RLRQ, c. C-1.1, art. 22 et 27.

	Année	Noms des lois	Irresponsabilité de principe	Article ou Section	Jurisprudence (exemples)	Commentaires
International	2020	ACEUM[25]	Oui	19.17	RAS	Texte très exonérant.
Europe	2001	Directive européenne[26]	Oui	Section 4: 12-15	Très fournie	Jurisprudence partagée, les juges étant parfois réticents à appliquer une exonération à des organisations qui ne sont pas toujours vues comme des intermédiaires techniques.

1.2.1.2 Densification progressive (2010 – …)

En dépit de ces débuts, les États se sont rendu compte que les marchés émergents donnaient place à une industrie dont la puissance de certains joueurs devenait importante, dopée par une globalisation croissante. Presque du jamais vu[27] ! Pourtant, ce phénomène aussi mondial soit-il, donne lieu à une réaction de régulation qui est sensiblement différente selon les espaces régionaux. Minimalement, sur le spectre des possibles, deux positionnements distincts peuvent être aperçus : l'Europe et l'Amérique.

1.2.1.2.1 Influence de l'Europe: une densification assumée

« Effet Bruxelles ». L'Europe, en matière de numérique, opte pour une approche clairement interventionniste. Aussi, si le continent ne constitue pas ce qui pourrait être considéré comme un « meneur » dans le développement de tels produits, elle souhaite imposer un « standard » élevé en matière de réglementation. Cette approche est d'ailleurs dénommée l'« effet Bruxelles »[28]. Si la démarche est ancienne et date des années 1990, avec notamment la Directive européenne de 1995 en matière de vie privée[29], elle s'est accentuée en matière de vie privée avec le RGPD[30], mais plus

---

25 *Accord Canada–États-Unis–Mexique (ACEUM)*, chapitre 19, Commerce numérique, art. 19.17, en ligne : <https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cusma-aceum/text-texte/19.aspx?lang=fra>.

26 Directive 2001/29/CE sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information.

27 James BESSEN, *The New Goliaths : How Corporations Use Software to Dominate Industries, Kill Innovation, and Undermine Regulation*, Yale, 2022. L'auteur affirme notamment que les technologies étant de plus en plus complexes (*supra*, Partie 1A i), son accessibilité est rendue impossible auprès de plus petites structures. Le temps de l'innovation disruptive n'est plus.

28 Anu BRADFORD, The Brussels Effect : How the European Union Rules the World, New York, OUP, 2020.

29 Directive 95/46/CE 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.

30 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.

récemment et plus généralement avec le paquet législatif de 2022[31]. On peut aussi penser au Règlement EIDAS[32] de 2014 qui a eu un effet mondial en matière de sécurité et d'identité, notamment à travers la récente Loi type de la CNUDCI sur le sujet[33] dont l'inspiration est importante.

Contrôle de marché. Parmi les éléments de distinction que nous sommes susceptibles d'identifier, au moins deux doivent être présentés. En premier lieu, comme mentionné précédemment, un questionnement en est un de marché que l'on souhaite en Europe réguler et notamment pour les très grosses structures commerciales[34]. Cet enjeu se manifeste surtout en lien avec les questions de protection des renseignements personnels (notamment le RGPD) et de droit de la concurrence (notamment le DMA).

Contrôle administratif lourd. La plupart des cadres de régulation européens se caractérisent par un support administratif significatif afin de s'assurer du respect préalable des règles. C'est là qu'apparaît une distinction importante entre la vision européenne et l'approche nord-américaine. La vision européenne favorise une approche *ex ante* où, forte d'un contrôle préalable d'une instance publique ou parapublique, une reconnaissance préalable est offerte à un acteur privé. Par exemple, une compagnie de certification pourra attester de la qualité de ses services de signature, car son système a été accrédité par un organisme dédié. L'approche *ex post*, beaucoup plus commune en Amérique, fait en sorte que le même acteur aura besoin de la validation d'un juge, par exemple, pour valider son niveau de qualité[35]. Une différence d'approche que l'on retrouve aussi dans la *Législation sur l'intelligence artificielle* ou avec les DMA et DSA.

DSA en résumé. Adopté en 2022, le *Digital Services Act* régit les services numériques et les plateformes numériques tels que les réseaux sociaux, les moteurs de recherche et les places de marché en ligne. L'État ajoute des obligations aux grandes plateformes pour lutter contre les contenus illégaux, les contenus nuisibles et les contrefaçons dans le but de protéger les droits des utilisateurs et de rendre les plateformes plus transparentes concernant leurs politiques de modération de contenu et leurs algorithmes.

---

31 Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (DSA); Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (DMA); Règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union (*COM(2021)0206* – C9-0146/2021 – *2021/0106(COD)*) (AIA).

32 Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.

33 A/CN.9/1112 - Projet de loi type sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance.

34 DMA et DSA s'appliquent aux structures qui disposent d'une influence sur 10 % de la population européenne.

35 Voir à ce sujet la différence qui prévaut dans la récente Loi-modèle de la CNUDCI entre les articles 23 (ex post) et 24 (ex ante).

DMA en résumé. Adopté en 2022 et suivant le mouvement d'encadrement législatif des grandes entreprises, le *Digital Market Act* concerne spécifiquement les grandes plateformes qui exercent une influence déterminante sur l'économie numérique. Cette Loi prévoit une liste d'interdictions spécifiques et de mesures correctives pour remédier aux pratiques anticoncurrentielles que les grandes plateformes devront respecter. De plus, le *Digital Market Act* désigne des autorités spécifiques pour superviser son application.

AI Act en résumé. En cours d'adoption en 2023, le *EU AI Act* prévoit des règles plus ou moins strictes dépendamment du niveau de risque des systèmes d'intelligence artificielle. Dans cette Loi, certains systèmes d'IA sont interdits à cause de leur atteinte aux droits fondamentaux tels les systèmes de surveillance social automatisée. De plus, l'*AI Act* propose la création d'une structure administrative, un organisme de régulation chargé de surveiller la mise en œuvre de la législation dans l'Union européenne.

1.2.1.2.2 Influence des États-Unis : une densification contrôlée

État des lieux. Face à la logorrhée législative européenne, la situation américaine est passablement différente. Aux États-Unis, au-delà de rares textes qui ont été adoptés sur des sujets assez précis[36], il est possible d'identifier soit des projets de lois[37], dont certains peuvent être vus comme isolés, voire un peu fantaisistes[38], soit des documents de nature éthique[39] qui sont donc peu impliquants juridiquement. Plusieurs projets de lois peuvent être envisagés comme étant assez timides quant aux obligations imposées[40].

Situation canadienne. La situation canadienne est un peu intermédiaire, entre États-Unis et Europe, c'est-à-dire entre passivité législative et adoption très dense. Au Canada d'abord, on constate une énergie modérée à adopter de nouveaux textes et si le projet fédéral C-27 est actuellement à l'étude, il faut d'abord dire que cela fait près de quatre ans que le processus législatif est engagé (C-11 précédant l'actuel C-27), et qu'une adoption ne semble pas prévue à très court terme. Ensuite, C-27 est encore assez préliminaire, d'abord parce que des adaptations importantes sont encore à venir,

---

36 On peut notamment citer la Loi californienne en matière de protection des renseignements personnels (California Consumer Privacy Act of 2018 (Title 1.81.5 added by Stats. 2018, Ch. 55, Sec. 3.).

37 Chris COONS, « Senator Coons, Colleagues Introduce Legislation to Provide Public with Transparency of Social Media Platforms », Press Release, December 21, 2022.

38 Certains projets de loi étatsuniens sont à l'initiative d'un seul parlementaire et peuvent parfois être vus plus comme un moyen de montrer le positionnement de ce dernier sur un sujet à la mode.

39 Notamment en matière d'intelligence artificielle. Voir aussi en matière de blockchain (National Archives, Blockchain White Paper, 2019, en ligne : <https://www.archives.gov/files/records-mgmt/policy/nara-blockchain-whitepaper.pdf>; Office of Financial Regulation of Florida, Assessment of Commerce and Regulatory Issues Presented by Blockchain Technology and Virtual Currency, 2022, en ligne : <https://flofr.gov/sitePages/documents/OFR-Blockchain-Technology-and-Virtual-Currency-Whitepaper-PRINT.pdf>).

40 Voir par exemple sur la technologie blockchain, le Senate Bill 4760/House Bill 8950, known as the *Digital Commodities Consumer Protection Act* of 2022, S. 4760, 117th Cong. (2022) qui ne fait que demander un registre des prestataires ainsi que le respect de « core principles ». Même chose avec le Executive Order 14067, Ensuring Responsible Development of Digital Assets (Exec. Order No. 14067, 87 C.F.R. § 49 (14143-14152)).

adaptations qui n'ont pas encore été déposées[41], mais aussi parce que ce projet de loi délègue une partie importante des exigences à de futurs règlements. À ce stade, il est donc difficile de pleinement évaluer la force à donner à ce texte. D'ailleurs, face à ces faibles avancements, un Code de conduite vient d'être adopté en septembre 2023[42]. Quant au Québec, outre certains changements assez ponctuels[43], la mise à jour la plus importante a été la Loi 25 en matière de renseignements personnels qui est venue adopter une approche assez proche du RGPD européen. À part cela, le technologique n'a que peu fait l'objet de changements d'envergure depuis 2001[44].

Adoption législative difficile. À ce sujet, au-delà du rapport à la loi qui est différent, il faut sans doute remarquer la plus grande difficulté à adopter des lois. Au Canada, les exemples sont multiples, notamment dans le domaine du numérique. La réforme du droit d'auteur de 2012 est intervenue plus de 10 ans après la vague principale des autres pays au début des années 2000. Le processus de mise à jour de la loi fédérale sur la vie privée[45] est laborieux au gré des changements de gouvernement, tout comme l'actuel C-18 qui a finalement reçu la sanction royale en juin 2023[46].

Tendance édulcorée. Pour le moment, et même si un discours d'apparence semble confirmer une densification des obligations de part, notamment pour les plus gros joueurs de l'industrie, que ce soit en matière de concurrence[47] ou d'intelligence artificielle[48], il est difficile d'identifier clairement des textes formels qui confirment cette tendance. Comme souvent aux États-Unis, il y a loin de la coupe aux lèvres quand vient le temps de contraindre l'industrie. Une industrie mondiale d'ailleurs résolument étatsunienne. Pour illustrer ce fait, notons qu'il est intéressant de constater le discours de la Maison Blanche en matière d'intelligence artificielle où, à l'été 2023 (21 juillet), une

---

41 De récents développements en chambre montrent que plusieurs sujets demeurent à peaufiner. Voir, notamment, le Comité permanent de l'industrie et des technologies, 26 septembre 2023, en ligne : <https://parlvu.parl.gc.ca/Harmony/fr/PowerBrowser/PowerBrowserV2/20230926/-1/39921>.

42 Gouvernement du Canada, *Code de conduite volontaire visant un développement et une gestion responsables des systèmes d'IA générative avancés*, septembre 2023, en ligne : <https://ised-isde.canada.ca/site/isde/fr/code-conduite-volontaire-visant-developpement-gestion-responsables-systemes-dia-generative-avances>.

43 On peut notamment penser à la mise à jour de la *Loi sur la protection du consommateur* en 2006 pour les contrats à distance (art. 54.1 et ss.), à l'avènement de la *Loi édictant la Loi sur le ministère de la Cybersécurité et du Numérique et modifiant d'autres dispositions*, sanctionnée le 3 décembre 2021, en ligne : <https://www.publicationsduquebec.gouv.qc.ca/fileadmin/Fichiers_client/lois_et_reglements/LoisAnnuelles/fr/2021/2021C33F.PDF>.

44 Je me permets de citer le Projet de loi 34 : Lo*i visant à moderniser la profession notariale et à favoriser l'accès à la justice* (2023), en ligne : <https://www.cnq.org/wp-content/uploads/2023/09/310719-PL-34_assemblee_nationale.pdf>.

45 Projet de loi C-27 : Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois, juin 2022.

46 Loi concernant les plateformes de communication en ligne rendant disponible du contenu de nouvelles aux personnes se trouvant au Canada (juin 2023).

47 Cela fait notamment référence aux débats parlementaires du Sénat étatsunien à l'été 2022 où un relatif consensus semblait de mise sur une hausse significative des obligations de la part des GAFAM.

48 On peut mentionner le projet de loi H.R.6580 - Algorithmic Accountability Act of 2022 proposé par quelques parlementaires qui présente certains éléments de contraintes, en ligne : <https://www.congress.gov/bill/117th-congress/house-bill/6580/text>.

démarche résolument volontaire est de mise[49]. Une certaine complaisance est pour le moment perceptible dans le fait que s'il y a bien concertation avec l'industrie et que le besoin d'un cadre pour une intelligence artificielle responsable est revendiqué, le temps des contraintes n'est pas encore venu.

1.2.2 Tendances et spécificités des approches juridiques

Des objets et des lois. Les objets à encadrer par les lois deviennent de plus en plus complexes. La généralisation accompagnée de la diversification des objets techniques a aussi engendré des besoins pour des lois plus complexes et plus diversifiées.

1.2.2.1 Tendances vers plus de complexité

1.2.2.1.1 Complexité de l'objet d'analyse

Complexité en général. La complexité que les technologies apportent a déjà été soulevée[50]. Notamment associée à l'opacité qui caractérise souvent le numérique[51], que cette dernière soit volontaire (entente de confidentialité), intrinsèque (explicabilité) ou causée par l'analphabétisme des interprètes[52], il est de plus en plus difficile de circonscrire une matière mouvante[53]. Forcément, cette complexité se répercute dans la façon de dire et d'appliquer le droit. Le numérique en général est à juste titre vu comme technique, forcément, impliquant par le fait même un dialogue entre des professions qui n'ont pas toujours l'habitude de se côtoyer. La donne est ensuite exacerbée par le fait que les questions sont nouvelles et que les appétits qui forcément surgissent doivent faire l'objet d'arbitrage entre des intérêts catégoriels distincts. Les débats sont de surcroît très souvent envisagés à une échelle internationale, ce qui implique des divergences de perspectives. Au-delà de la nouveauté, il apparaît clairement que le domaine est évolutif et diffère d'une année à l'autre.

Technologie. Face à la complexité constatée, et pour évacuer ce questionnement, il nous semble que le terme de « technologie de l'information » que l'on retrouve dans le titre a bien vieilli dans la mesure où il se comprend comme un support résiduel qui s'appose à ce qui n'est pas tangible. Les « nouvelles » technologies, comme l'intelligence artificielle connexionniste ou les chaînes de blocs, peuvent donc sans difficultés être incluses sous ce vocable. Aussi, au-delà de la double acceptation entre le support et le format[54], la terminologie ne pose pas de difficulté à intégrer la nouveauté et la complexité qui vient avec.

---

49 Voir notamment *White House, Ensuring Safe, Secure, and Trustworthy AI*, juillet 2023, en ligne : <https://www.whitehouse.gov/wp-content/uploads/2023/07/Ensuring-Safe-Secure-and-Trustworthy-AI.pdf>.

50 *Supra*, Section 1.1.1.2.

51 *Supra*, Section 1.1.2.2.

52 Pour reprendre la dichotomie proposée par J. BURELL, « How the Machine "thinks": Understanding Opacity in Machine-Learning Algorithms », (2016) 3-1 *Big Data and Society* 1, 3-4.

53 Cette situation de complexité est notamment reconnue dans la jurisprudence elle-même où certains juges, assez candidement, expriment leur difficulté à cerner la technique qu'ils doivent apprécier. *R.* c. *Veillette*, 2016 QCCQ 15192, para. 41; *R.* c. *Avanes*, 2019 ONCJ 606, para. 32.

54 Vincent Gautrais, *Étude juridique sur la Loi concernant le cadre juridique des technologies de l'information* (RLRQ c C-1.1) – Mandat du ministère de la Justice du Québec, 31 juillet 2020, para. 3.2.1.1.

Complexité plus spécifique au domaine d'application de la LCCJTI. Mais ce n'est pas tout. En vingt ans, les technologies se sont densifiées et elles autorisent désormais des actions qui n'avaient pas alors été considérées. Le meilleur moyen de s'en rendre compte est d'envisager le spectre des possibles tel que décrit dans la LCCJTI et qui s'articule autour des six opérations décrites à l'article 6. Ainsi, un document peut être : créé; transféré; consulté; archivé; détruit[55].

Dites différemment, les opérations qui sont envisagées dans la LCCJTI sont :

- le transfert[56];
- la conservation (qui comprend notamment l'hébergement et la garde)[57];
- la consultation[58];
- la communication[59].

Or, vingt ans plus tard, il y a des opérations qui n'avaient pas été considérées. Ou si peu... Prenons l'exemple de l'automatisation qui devient désormais possible avec la généralisation de l'intelligence artificielle. Outre le spectre très limité de l'article 35[60], qui envisageait le seul caractère transactionnel, le « traitement »[61], l'utilisation ou la circulation[62] des données que cette

---

55 Article 6 LCCJTI: « L'intégrité du document doit être maintenue au cours de son cycle de vie, soit depuis sa création, en passant par son transfert, sa consultation et sa transmission, jusqu'à sa conservation, y compris son archivage ou sa destruction ».

56 Art.17 et ss.

57 Art. 19 et ss.

58 Art. 23 et ss.

59 Art. 28 et ss.

60 Art. 35: « la partie qui offre un produit ou un service au moyen d'un document préprogrammé doit, sous peine d'inopposabilité de la communication ou d'annulation de la transaction, faire en sorte que le document fournisse les instructions nécessaires pour que la partie qui utilise un tel document puisse dans les meilleurs délais l'aviser d'une erreur commise ou disposer des moyens pour prévenir ou corriger une erreur. De même, des instructions ou des moyens doivent lui être fournis pour qu'elle soit en mesure d'éviter l'obtention d'un produit ou d'un service dont elle ne veut pas ou qu'elle n'obtiendrait pas sans l'erreur commise ou pour qu'elle soit en mesure de le rendre ou, le cas échéant, de le détruire ».

61 Le terme « traitement » est inclusif, mais il est connoté dans la mesure où c'est celui qui prévaut en matière de protection des renseignements personnels en Europe. En revanche, dans un contexte québécois, il semble beaucoup plus facile à utiliser dans le sens que nous souhaitons lui donner ici dans la mesure où il n'est que peu utilisé en matière de protection des renseignements personnels au Québec, les lois préférant distinguer les diverses opérations (collecte, communication, conservation, utilisation). Pour conforter ce sens générique au terme de traitement que l'on trouve au Québec, voir *L.D.* c. *Commission de la construction du Québec*, 2017 QCCAI 34, para. 20. Voir aussi OQLF, *Vocabulaire du traitement de données*, en ligne : <https://www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/vocabulaire-traitement-donnees.aspx> qui définit le traitement de cette façon : « Ensemble des opérations que les ordinateurs d'un système informatique peuvent effectuer sur des données dans le but de les transformer en ressources exploitables ».

62 Pour reprendre l'expression utilisée dans Vincent GAUTRAIS et Pierre TRUDEL, *Circulation des renseignements personnels et Web 2.0*, Thémis, Montréal, 2010. Par rapport à ce titre, on peut dire que, 13 ans plus tard, la référence au « Web 2.0 » est datée, du fait de sa non-neutralité technologique, mais pas celle de « circulation ».

technologie requiert n'avait que peu été envisagée[63]. Le fait de « faire parler les données », comme l'autorise désormais l'intelligence artificielle, n'est pas considéré dans la Loi comme une opération en tant que telle. Cette non-intervention de la LCCJTI est normale au regard de l'état des pratiques en 2001, mais sans doute dommageable aux regards des risques en 2023. En fait, notons que la Loi a donné lieu à quelques changements mineurs en 2021 avec le Projet de loi 6 qui, selon les dispositions relatives au Comité d'harmonisation, évoque désormais le terme générique d'« utilisation des technologies ».

Du document aux données. Un autre élément d'évolution, et sans doute de complexification, est que si la Loi est structurée autour de la notion de document, la tendance universelle est de considérer désormais la donnée comme objet premier d'analyse autour de laquelle les textes législatifs organisent leur encadrement. Cela dit, la donnée est envisagée comme une composante symbiotique du document[64], la seconde étant nécessaire au premier. Plus exactement, dans la Loi, la donnée est envisagée sous le terme synonymique d'information. Or, il est d'autant plus facile d'assimiler ces deux notions dans le cadre de cette Loi, dans la mesure où il est habituel de considérer que l'information est une donnée structurée, contextualisée[65], et que justement l'information à l'article 3 de la LCCJTI évoque spécifiquement le besoin que l'information soit ainsi structurée. Pour toutes ces raisons, nous croyons que l'ajout de l'opération de « traitement » tel qu'expliqué précédemment, permet de considérer les problématiques généralement associées aux données.

PROPOSITION #1 : Si la notion de « technologie » semble particulièrement adaptée 20 ans plus tard, le spectre des opérations susceptibles d'être envisagées est en revanche désormais trop étroit. On pourrait donc envisager l'hypothèse de « traitement » comme nouvelle situation demandant un régime d'encadrement.

1.2.2.1.2 Complexité du droit

Cette complexité inhérente se répercute forcément dans la manière de réguler. Comme dans le domaine de l'environnement, le fait de : « répondre au technique par le technique – a donc favorisé la complication juridique et la complexité d'un droit qui par ailleurs combine à l'infini les sources, nationales, européennes et internationales »[66].

---

63 Outre néanmoins les données en lien avec les « caractéristiques personnelles » que l'on trouve aux articles 40 à 45.

64 Art. 3 de la *Loi*.

65 Il est de commune renommée que la donnée est un fait brut alors que l'information est une donnée mise en contexte, interprétée. Voir Nicolas VERMEYS *et al.,* « Étude relative à l'incidence des technologies de l'information et des communications sur la gestion de l'information dans l'administration judiciaire québécoise », étude présentée au ministère de la Justice du Québec, 2017, p. 11 : « Les données sont des signes ou des ensembles de signes dénués de sens et isolés les uns des autres. Elles sont la base à partir de laquelle l'information se construit. L'information serait donc une association de données, qui, liées les unes aux autres, sont créatrices de sens ».

66 Véronique LABROT, « Droit et complexité : regard sur le droit de l'environnement », dans Mathieu DOAT, Jacques LE GOFF et Philippe PÉDROT (dir.), *Droit et complexité: pour une nouvelle intelligence du droit vivant*, Rennes, Presses Universitaires de Rennes, 2007, p. 17, à la page 20.

Il est donc possible de se demander, au même titre que l'on fait les auteurs Lessig[67] et Easterbrook[68] dans les années 1990, se répondant l'un l'autre, si le droit du numérique présente des spécificités ? Notre tendance est de dire, minimalement pour les matières techniques[69], que certaines spécificités apparaissent. Sans prétention d'exhaustivité, nous aimerions citer justement celle de la complexité. Une complexité qui se comprend parfois par la remise en cause des structures organisationnelles traditionnelles, comme dans la situation de la blockchain et sa forme décentralisante[70], parfois dans la substance même du droit qui demeure mal connue, voire absente[71]. Sans souscrire à la prétention souvent affirmée à tort du vide juridique, il n'en reste pas moins que les acteurs ne disposent que de peu de guides quant à la manière de signifier leur diligence numérique. La complexité se traduit aussi par le recours désormais systématique à des normes techniques nécessitant des documentations internes.

1.2.2.2 Tendances vers plus de diversification des normes

À cet égard, on peut affirmer que le modèle classique de droit positif, basé sur une hiérarchie des normes où un rôle prépondérant est alloué à la loi, a quelque peu vécu. Plus exactement, il est de bon ton de plébisciter une vision plus plurielle, en connexion de ce que certains appellent « l'École de Montréal », celle-ci se vérifie en pratique où les lois réfèrent à des décrets qui réfèrent à des normes techniques qui réfèrent à des documentations internes. Une délégation multiple est donc de mise[72], générant des « espaces d'interrégulation »[73] avec lesquels nous n'avons pas tant de recul. D'autant que cette double délégation implique une intervention de différentes disciplines, certaines normes dites techniques étant souvent incompréhensibles pour le commun des juristes. Quoi qu'il en soit, il importe, comme juriste, comme gouvernement, de s'intéresser à ces trois niveaux de ce « mille-feuilles normatif »[74]. L'intérêt pour ces niveaux plus bas de la normativité (normes informelles et individuelles) est d'autant plus justifié que des doutes subsistent, tant sur leur contenu que sur l'existence de ces règles[75].

---

67 Larry LESSIG, « The Law of the Horse. What Cyberlaw Might Teach », (1999) *Harvard Law Review* 501.

68 F. H. EASTERBROOK, « Cyberspace and the Law of the Horse », University of Chicago Legal Forum, 1996, n° 1, p. 207.

69 D'où les comparaisons avec le droit de l'environnement et de la santé.

70 Voir notamment le propos critique d'Alain Supiot sur la disparition du rôle du tiers. Alain SUPIOT, « Le crédit de la parole », *Le grand continent*, 1er août 2022, en ligne : <https://legrandcontinent.eu/fr/2022/08/01/le-credit-de-la-parole/>.

71 Encore au regard de la comparaison entre droit du numérique et de l'environnement, lire Véronique LABROT, « Droit et complexité : regard sur le droit de l'environnement », dans Mathieu DOAT, Jacques LE GOFF et Philippe PÉDROT (dir.), *Droit et complexité: pour une nouvelle intelligence du droit vivant*, Rennes, Presses Universitaires de Rennes, 2007, p. 17, à la page 22.

72 Vincent GAUTRAIS et Henry LAVILLE, « Pour une gouvernance participative des données personnelles au Québec », dans Cyril SINTEZ (dir.), *Mélanges Catherine Thibierge*, Mare et Martin, Paris, 2023, p. 199.

73 M.-A. FRISON-ROCHE (dir.), *Internet, espace d'interrégulation*, Paris, Dalloz, 2016.

74 *Infra*, Section 2.1.1.1.1 sur l'éventuel nouveau rôle du Comité d'harmonisation.

75 AI Institute, « Algorithmic Accountability : Moving Beyond Audits », 11 avril 2023 : « There is a burgeoning audit economy with companies offering audits-as-a-service despite no clarity on the standards and methodologies for algorithmic auditing, nor consensus on the definitions of risk and harm ».

1.2.2.3 Tendances diverses selon les spécificités culturelles

Traditions culturelles. Le Québec se trouve au carrefour des traditions culturelles nord-américaines et européennes. Cela se reflète sur les approches juridiques qui sont susceptibles d'y être retenues.

1.2.2.3.1 Selon la prévalence à utiliser des institutions

Exemple de protection des renseignements personnels. Si la réflexion sur le numérique est globale, l'application du droit est directement associée à la juridiction concernée. L'exemple le plus emblématique de cette influence d'un pays à l'autre est le droit de la protection des renseignements personnels où l'avènement du RGPD est directement à l'origine de l'adoption de la Loi 25. En effet, et même si la densification des règles en la matière est assez universelle, du fait des nouveaux risques précités[76], un avis de 2014 de la Commission européenne[77] avait souligné quelques manquements afin que le Québec puisse être considéré comme une juridiction ayant un niveau de protection équivalent[78]. Dans ce cas précis, un choix politique a clairement été pris où une certaine inclinaison avec l'approche européenne semble perceptible sur ce domaine de droit en particulier. Cela dit, au-delà de ces sources d'harmonisation, il n'en demeure pas moins que des spécificités demeurent d'une juridiction à l'autre.

Cadre administratif. Sur le plan institutionnel, conséquence d'une place de l'État différente, il reste à prévoir que la mise en application de la Loi 25 ne s'opère pas de même manière que le RGPD. Ce dernier prévoit en effet différentes structures qui sont en mesure tant d'appliquer le droit que de proposer des cadres normatifs qui puissent servir de guide aux différents acteurs[79]. Il en va de même du règlement européen sur l'intelligence européenne qui identifie différents acteurs qui sont en mesure aussi bien de sanctionner que de servir de guide[80]. Même si, concernant les renseignements personnels, une certaine « réinstitutionalisation » semble de mise, notamment avec une hausse du budget de la CAI du fait de ses nouvelles obligations, la place de l'État n'est peut-être pas aussi présente en Amérique qu'en Europe. Guy Rocher, par exemple, évoquait qu'en Amérique du Nord « la démocratie est plus horizontale que la démocratie républicaine »[81].

Comité d'harmonisation. D'ailleurs, plus proche de nous, le comité d'harmonisation prévu aux articles 63 et suivants de la Loi était un espace qui aurait pu permettre à l'État de participer

---

76 *Supra*, Section 1.1.

77 Groupe de travail sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel, Avis 7/2014 sur la protection des données à caractère personnel au Québec, 4 juin 2014, en ligne : <https://www.dataprotection.ro/servlet/ViewDocument?id=1290>.

78 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, article 45.

79 Vincent GAUTRAIS, « Made in Canada : distinctions culturelles de la protection des renseignements personnels canadienne », (2021) 33-3 *Cahiers de propriété intellectuelle* 1365, en ligne : <https://www.lescpi.ca/articles/v33-v33-volume-33-numero-3/made-in-canada-distinctions-culturelles-de-la-protection-des-renseignements-personnels-canadienne/>.

80 *Id.*

81 François ROCHER, *Guy Rocher : entretiens*, Montréal, Boréal, 2010, p. 114.

davantage à l'élaboration des règles applicables. Au meilleur de notre connaissance, il n'a que peu joué ce rôle[82]. Cela dit, quelques changements récents pourraient laisser croire à une densification de son rôle[83].

1.2.2.3.2 Selon les valeurs associées au Québec

Différences substantielles. Au-delà de ces différences institutionnelles, il existe aussi avec l'Europe des distinctions substantielles. Évidemment, si l'Europe constitue une source importante d'inspiration sur la régulation du numérique, il n'en demeure pas moins qu'il importe de ne pas sous-estimer les différences qui existent aussi à cet égard. La protection de la protection des renseignements personnels en est un bon exemple, que ce soit en ce qui a trait à la notion de traitement[84], de droit à l'oubli[85], de publication des décisions de justice[86], etc. Après, il ne faut pas sous-estimer non plus l'inspiration profonde que constitua le RGPD en droit de la protection des renseignements personnels au Québec. En effet, plusieurs dispositions de ce règlement européen ont eu un effet direct sur la Loi 25. On peut notamment penser aux sanctions précitées qui sont au Québec, mais aussi au Canada, une inspiration directe de l'approche plus directive de l'Europe. À certains égards, on peut croire que le poids relatif du Québec sur l'échiquier mondial fait qu'il est parfois plus réaliste de suivre la tendance internationale.

Exemple des plateformes. De façon plus générale, les différences substantielles sur la régulation du numérique entre l'Europe et le Québec sont surtout associées au fait que la première juridiction a adopté une série de lois sur le sujet, alors que l'encadrement est passablement plus « humble » au Québec. On peut notamment citer le cas de certaines plateformes mondiales bien connues qui ont suscité des réactions législatives pour le moment assez tièdes[87], surtout en comparaison des derniers textes européens particulièrement incisifs[88].

---

82 Vincent GAUTRAIS, *Étude juridique sur la Loi concernant le cadre juridique des technologies de l'information* (RLRQ c C-1.1) – Mandat du ministère de la Justice du Québec, 31 juillet 2020, p. 78 et ss., notamment la proposition 24.

83 *Infra*, 2.1.1.1.

84 Au Québec, et au Canada, la structure des lois en matière de protection des renseignements personnels s'articule selon le type d'opération concerné et non au regard de la notion englobante de « traitement » qui prévaut en Europe.

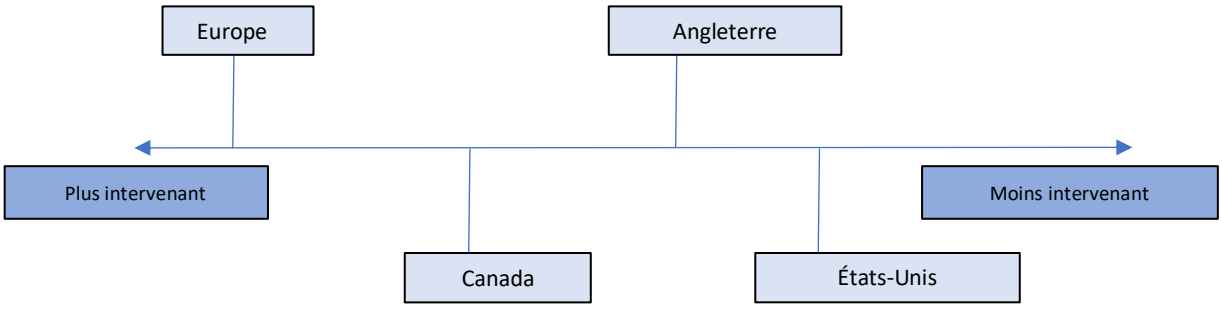
85 Si le droit à l'oubli tel que prévu dans la Loi 25 est d'inspiration européenne, les modalités de la mise en application (prévues à l'art. 88 de la LAPRPSP et 40 de la LPRPSP) sont sensiblement différentes de celles prévues dans le RGPD.

86 *Sherman (Succession)* c. *Donovan*, 2021 CSC 25. Au Québec, on peut notamment penser à la pratique de la Commission d'accès à l'information (CAI) qui depuis le 1er décembre 2017 n'anonymise plus systématiquement ses propres décisions.

87 Au-delà de la Loi qui n'a que peu été modifiée depuis 2001, on peut citer : de rares dispositions pour encadrer un peu les plateformes de transport de personnes (approche minimaliste) dans la nouvelle *Loi concernant le transport rémunéré de personnes par automobile*, par exemple; de rares dispositions pour encadrer les plateformes d'hébergement dans la *Loi sur l'hébergement touristique*

88 *Supra*, 1.2.1.2.1.

1.2.2.3.3 Illustration



Différences étatiques dans la manière de réguler l'IA. En matière d'intelligence artificielle, comme nous l'avons montré plus généralement il y a quelques pages, il existe un spectre de possible très vaste entre l'approche interventionniste européenne et le laisser-aller étatsunien. À certains égards, et même s'il n'est encore qu'à l'étape de projet de loi, le projet C-27 est relativement ambitieux, souhaitant notamment mettre en place des institutions dédiées à ce sujet, contrairement à l'Angleterre qui préfère partager les ressources avec une pluralité d'organisations existantes[89].

1.2.3 Tendances fonctionnelle et neutre des approches juridiques

Effectuer une évaluation de la LCCJTI 20 ans plus tard impose de regarder comment ont évolué sans doute les deux concepts les plus fondamentaux en termes de rédaction des lois : l'équivalence fonctionnelle et la neutralité technologique. Deux notions qui sont omniprésentes dans la Loi; deux notions qui ne sont pas sans lien et qui sont souvent associées à deux côtés d'une même pièce.

1.2.3.1 Tendance fonctionnelle

1.2.3.1.1 Description de l'approche fonctionnelle

Notion « reine ». La LCCJTI est un texte qui a centré tant sa substance que sa structure sur l'approche fonctionnelle. Sur le plan de la substance, on la retrouve, notamment, dès l'article 1[90]. Au niveau de la structure, elle peut être trouvée dans les titres mêmes de la Loi qui traite de notions qui sont indépendantes tant des supports (analogique ou numérique) que des technologies (format).

Pertinence maintenue. Même si la notion d'équivalence fonctionnelle était sans doute plus à la mode il y a 20 ans que maintenant[91], originant notamment des travaux de la CNUDCI, il n'en demeure pas moins que cette approche utilisée aussi pour rédiger les lois nous semble pleinement applicable pour encadrer la nouvelle réalité technologique. Ainsi, les manières de faire qui avaient cours « à l'époque » du papier constituent une sorte de « mètre étalon » dans l'organisation du numérique. De surcroît, cette comparaison ne s'opère pas comme un calque trop rigide, mais en

---

89 Voir notamment : Teresa SCASSA, « Comparing the UK's Proposal for AI Governance to Canada's AI Bill », 14 avril 2023, en ligne : <http://www.teresascassa.ca/index.php?option=com_k2&view=item&id=370:comparing-the-uks-proposal-for-ai-governance-to-canadas-ai-bill&Itemid=80>.

90 Art. 1 (3) LCCJTI.

91 Nous entendons par là que les nouveaux textes tant européens qu'américains sur lesquels nous basons la présente étude ne vont souvent pas explicitement référer à cette notion.

s'intéressant aux fonctions que l'on souhaite garantir, autorisant aux juges la capacité d'interpréter et ainsi d'adapter le droit aux faits.

Tous les supports. Suivant cette approche, il est possible de croire que la Loi s'applique à tous les supports, que ceux-ci soient analogiques (physiques ou tangibles) ou technologiques. En dépit de son titre, qui réfèrent aux technologies de l'information, elle traite à plusieurs reprises de situations ou circonstances qui sont clairement physiques. À titre d'exemple, le chapitre 2 (art. 3 à 37) traite des « Documents » et ne fait pas toujours une distinction entre les supports. Il en va de même de certaines opérations, comme la conservation et la transmission, qui peuvent être assurées par tous les supports. Cet état de fait s'explique sans doute en partie du fait de l'approche fonctionnelle précitée, dans la mesure où l'on compare le technologique au physique préexistant.

Toutes les technologies. L'équivalence fonctionnelle ne vaut pas que pour le support dont nous venons de parler (technologique par rapport au physique). Il vaut aussi pour la comparaison qui peut prévaloir entre deux technologies de l'information différentes (deux formats différents). Certes, une confusion prévaut sur la polysémie associée au fait que technologie concerne à la fois le support (de celui qui s'oppose au physique), mais aussi une composante du document. Certes, cette imprécision est problématique[92], d'autant qu'elle pourrait être amenuisée en qualifiant la seconde acception de « format »[93].

Sage comparaison. Cette manière de faire comparative nous semble sage. D'abord, elle autorise une approche plus analytique. Ensuite, la portée de la Loi est assez générique et, sauf exception, elle vise à encadrer un cadre commun qui est susceptible de s'appliquer à un grand nombre de situations. Cela n'empêchera pas de prévoir un cadre, par exemple, spécifique pour l'IA même s'il importe de justifier pourquoi un traitement indépendant s'impose. Encore, l'approche fonctionnelle présente la vertu d'une meilleure adaptation au temps[94].

Cas des caméras intelligentes. En 2023, sont apparues dans la presse québécoise des manchettes selon lesquelles une compagnie française cherchait à développer un marché pour une technologie de caméra dite intelligente qui permet, selon les dires de ladite compagnie, de lutter contre le vol à l'étalage[95]. Sans que l'on ne sache grand-chose sur ce procédé, on peut néanmoins constater que les articles 40 et ss. de la LCCJTI semblent applicables, le texte ayant pris le soin de ne pas traiter que de biométrie, technologie à la mode en 2001, mais plus généralement à un « document technologique qui présente une caractéristique personnelle » (art. 41) ou à une « banque de caractéristiques » (art. 45). Ensuite, il faut noter la souplesse de l'article 45 quant aux modalités de mises en application de tels procédés. En effet, cette disposition identifie l'obligation de produire une documentation qui doit être déposée à la CAI, le tout sans empêcher la mise en place dudit

---

92 Vincent GAUTRAIS, *Étude juridique sur la Loi concernant le cadre juridique des technologies de l'information* (RLRQ c C-1.1) – Mandat du ministère de la Justice du Québec, 31 juillet 2020, p. 34. Cette étude s'était notamment basée sur un sondage où 85 % des personnes interrogées pensaient que cette ambivalence était problématique et devait être corrigée.

93 *Id.*, propositions 1 et 2, p. 36.

94 Chris Reed, « Taking Sides on Technology Neutrality », (2007) 4-3 *Script-ed* 263, 266.

95 Tristan PÉLOQUIN, « Quand l'intelligence artificielle vous épie à la pharmacie », (6 février 2023) *La Presse*, en ligne : <https://plus.lapresse.ca/screens/d7fb0fec-d831-47e2-9a38-590ed8cf8c18%7C_0.html>.

procédé. Cette démarche n'est de surcroît pas sans conséquence, la CAI ayant un vrai pouvoir de sanction pouvant aller jusqu'à l'interdiction du développement. Les dispositions de 2001 s'appliquent assez harmonieusement à une technologie de 2023.

1.2.3.1.2 Approche fonctionnelle dans les démarches législatives récentes

Comme mentionné plus tôt, si l'équivalence fonctionnelle est moindrement considérée et citée[96], elle demeure applicable pour encadrer juridiquement les technologies.

CNUDCI. Il est important de regarder ce que la CNUDCI pense de cette notion dans la mesure où elle en est, sinon l'inventrice, mais au moins l'une des sources qui a grandement contribué à étendre son intégration dans les lois. Les récents travaux de cette institution évaluent la pertinence de l'équivalence fonctionnelle, et si elle demeure majeure, elle n'est peut-être pas, peut-être plus, ce principe sans faille qui trouvait à s'appliquer.

> « L'approche d'équivalence fonctionnelle présuppose l'existence d'exigences légales qui prévoient directement ou indirectement l'exécution d'une opération physique ou sur papier, telle que l'utilisation d'un justificatif papier pour identifier une personne ou une communication papier pour authentifier un fait ou une chose. Elle analyse ensuite les objectifs et les fonctions de ces exigences en vue de déterminer comment atteindre ces objectifs ou remplir ces fonctions par des moyens électroniques. Toutefois, tout comme la technologie numérique a rendu possible des activités qui n'ont pas d'équivalent papier, certains services de gestion de l'identité et certains services de confiance visés par le [projet d'instrument] n'ont peut-être pas d'équivalent papier. »[97] (Notre soulignement)

Cet extrait nous révèle plusieurs points. En premier lieu, au-delà de l'explication de ce qu'elle est, il semble qu'ici l'approche des équivalents fonctionnels vise la rédaction des lois et moindrement les hypothèses d'interprétation de celles-ci[98]. En deuxième lieu, il demeure que cette manière de rédiger les lois est toujours de mise. D'ailleurs, et même si cela apparaît dans d'autres endroits que celui précités, elle reste une des façons la plus commune en bâtissant le futur sur l'avenir. En l'occurrence, le numérique sur le physique. Simplement, près de quarante ans après l'avènement de cette approche, on semble reconnaître des hypothèses où la seule comparaison ne suffit plus. La CNUDCI identifie d'ailleurs clairement des situations où cette approche ne vaut « que si un équivalent de l'identification hors ligne existe »[99].

Ontario. Une illustration intéressante qui montre la pertinence de ce principe est l'Ontario, qui considère de réformer sa *Loi sur la protection des consommateurs*, quasiment inchangée depuis 2002. En 2002, justement, on se basait sur le principe d'équivalence fonctionnelle pour s'assurer

---

96 À la différence de la neutralité technologique qui est explicitement citée. *Infra*, 1.2.3.2.

97 CNUDCI, Note explicative sur le projet de dispositions relatives à l'utilisation et à la reconnaissance internationale de la gestion de l'identité et des services de confiance, A/CN.9/WG.IV/WP.171, 2022, para. 19.

98 Sur la distinction, Vincent GAUTRAIS, Neutralité technologique : Rédaction et interprétation des lois face aux changements technologiques, Montréal, Éditions Thémis, 2012.

99 CNUDCI, Note explicative sur le projet de dispositions relatives à l'utilisation et à la reconnaissance internationale de la gestion de l'identité et des services de confiance, A/CN.9/WG.IV/WP.171, 2022, para. 97.

que la vente en ligne bénéficie du même niveau de protection que les autres types de vente. Or, en 2023, un nouveau projet de loi est proposé qui recherche à instituer un régime uniforme.

> « The ministry is proposing to combine contract disclosure rules into a single set of core rules that would apply to most consumer contracts including direct, remote, internet, future performance, timeshare, personal development service, loan brokering, credit repair services and certain lease agreements. »[100]

Cette tentative d'uniformisation, qui se distance de l'approche d'équivalence fonctionnelle, est jugée sévèrement dans la mesure où une telle approche est susceptible de remettre en question certaines protections qui ont été introduites en 2002. Un rapport de la Commission des droits de l'Ontario semble en effet estimer, à raison, qu'une remise en cause de cette distinction serait susceptible de nuire à la protection du consommateur[101].

Illustrations. Il est néanmoins possible de croire que certaines situations vont moindrement donner l'occasion d'être encadrées au regard de ce principe rédactionnel. En effet, ce réflexe comparatif est plus difficile à envisager en ce qui a trait à la plateformisation des relations, le contexte présentant des éléments de changements substantiels.

PROPOSITION #2 : L'équivalence fonctionnelle est une notion clé largement utilisée dont la pertinence demeure. Il importe néanmoins d'analyser, selon la technologie que l'on cherche à encadrer, si le comparatif avec le support analogique est justifié.

1.2.3.2 Tendance et neutralité technologique

Notion toujours à la mode. Si la notion d'équivalence fonctionnelle demeure moins explicitement évoquée, celle de neutralité technologique demeure régulièrement utilisée. Il nous semble important de considérer cette notion dans la mesure où, alors qu'elle est surutilisée et invoquée dans les lois et normes récentes, elle pâtit d'une carence conceptuelle[102]. Un survol rapide des textes en droit du numérique montre qu'elle est revendiquée tant dans des textes européens[103], canadiens[104], qu'étatsuniens[105]. Un consensus s'opère à son endroit considérant donc que les lois

---

100 « Consultation Paper on Modernizing the Consumer Protection Act, 2002 », 23 février 2023, en ligne : <https://www.ontariocanada.com/registry/view.do?postingId=43452>.

101 Law Commission of Ontario, *Consumer Protection in the Digital Marketplace*, juin 2023, p. 38, en ligne : <https://www.lco-cdo.org/wp-content/uploads/2023/06/LCO-Consumer-Consultation-Paper-Updated-Final.pdf>.

102 Brad A. GREENBERG, « Rethinking Technology Neutrality », (2016) 100 *Minnesota Law Review* 1495, 1498 : « Technology neutrality is undertheorized and, thereby, poorly understood ».

103 eIDAS, considérants 16 et 27, art. 12; RGPD, considérant 15; AI Act (section 3.1 et 5.2.1).

104 Gouvernement du Canada, *Targeted Regulatory Review : Digitalization and Technology-Neutral Regulations Roadmap*, 2021, en ligne : <https://ised-isde.canada.ca/site/acts-regulations/en/forward-regulatory-plan/targeted-regulatory-review#s1>.

105 Cette qualité est revendiquée tant par l'industrie (comme une chambre de commerce, en ligne : <https://aithority.com/machine-learning/u-s-chamber-takes-strong-stance-for-technology-neutral-ai-laws-and-alliances/)> que par le gouvernement (White House, *Memorandum for the Heads of Executive Departments and Agencies*, 2020, en ligne : <https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf>, p. 5).

doivent s'appliquer, dans la mesure du possible, à l'ensemble des supports (analogique et technologique)[106] et à l'ensemble des technologies.

Notion « tarte aux pommes ». De la même manière, alors que la CNUDCI semble faire évoluer quelque peu le principe de l'approche de l'équivalence fonctionnelle, comme vu précédemment, elle n'entend pas remettre en cause la neutralité technologique. Pourtant, cette notion est souvent critiquée du fait de sa compréhension hasardeuse[107], aussi du fait que d'autres solutions soient parfois meilleures[108]. Elle n'a également que peu été considérée par les tribunaux[109]. Si la notion est source de quiproquo, elle est pourtant souvent employée; et bien que des contre-exemples existent, il est de commune renommée de penser qu'il est important de respecter ce principe[110]. Ce principe est donc certes dominant, comme s'il s'agissait d'un concept trop mou pour pouvoir s'en distancier : un effet « tarte aux pommes » pour reprendre l'expression d'un auteur[111]. Pourtant, il y a un revers de médaille à la toute-puissance de ce principe : le retrait de la part du législateur qui ne veut pas intervenir plus qu'il ne faut. Ce dernier a en effet eu une position relative de moindre intervention alors qu'il est tout à fait imaginable, c'est son rôle de vouloir légiférer spécifiquement dès lors qu'une technologie est susceptible de créer de nouveaux risques ou que de nouvelles valeurs veulent être mises de l'avant. On pense notamment à la récente Loi 3[112] qui prévoit spécifiquement un cadre particulier dans la mesure où, outre la protection des renseignements personnels qui est déjà présente dans la Loi 25, on souhaite valoriser les données de santé.

Discrimination technologique. De plus, comme en 2001, il est sans doute inévitable d'avoir des dispositions dans la LCCJTI qui touchent précisément certaines technologies. Ainsi, relativement à des questionnements plus ambitieux, plusieurs recommandent même qu'il importe d'adopter une telle approche[113]. Dans la mesure où, tel que nous l'avons déjà évoqué, les technologies ne sont pas neutres, il est envisageable au contraire de favoriser une approche « discriminante »[114] sur le plan technologique. D'abord, en favorisant l'analyse d'une telle approche, cela permet d'améliorer

---

106 La neutralité sur le support est aussi parfois dénommée la neutralité médiatique.

107 Vincent GAUTRAIS, Neutralité technologique : Rédaction et interprétation des lois face aux changements technologiques, Montréal, Éditions Thémis, 2012. Brad A. GREENBERG, « Rethinking Technology Neutrality », (2016) 100 Minesota Law Review 1495.

108 Paul OHM, « The Argument Against Technology Neutral Surveillance Laws », (2010) 88 *Tex. L. Rev*. 1685.

109 Une jurisprudence assez fournie existe en droit d'auteur au Canada, mais au meilleur de notre connaissance même si la notion existe dans la LCCJTI aucun jugement ne traite de front cette notion au regard de ce texte.

110 Brad A. GREENBERG, « Rethinking Technology Neutrality », (2016) 100 *Minesota Law Review* 1495.

111 Chris REED, « Taking Sides on Technology Neutrality », (2007) 4-3 *Script-ed 263*, 266. Comme l'auteur, l'un des objectifs majeurs de la présente discussion est : « attempts to analyse whether the general wisdom, that technology neutrality is unquestioningly as good a thing as motherhood and apple pie, is correct ».

112 Loi sur les renseignements de santé et de services sociaux et modifiant diverses dispositions législatives, sanctionnée le 4 avril 2023.

113 Paul OHM, « The Argument Against Technology Neutral Surveillance Laws », (2010) 88 *Tex. L. Rev.* 1685, 1687–1700. Brad A. GREENBERG, « Rethinking Technology Neutrality », (2016) 100 *Minesota Law Review* 1495.

114 Brad A. GREENBERG, « Rethinking Technology Neutrality », (2016) 100 *Minesota Law Review* 1495.

une application plus « fine » de la loi : « Technology specificity, in contrast, facilitates greater tailoring of the law »[115].

Ensuite, il est sans doute plus aisé de mesurer l'équilibre entre protection des intérêts en jeu et innovation[116]. Appliquant ce questionnement au seul droit d'auteur, Greenberg prétend que : « Coupled with increased tailoring, technological discrimination would help copyright law provide incentives for authors and facilitate innovation as a default, without relying so heavily on ad hoc fair use determinations »[117].

Neutralité technologique dans la LCCJTI. Si ce principe n'est pas explicitement prévu dans la LCCJTI[118], on peut néanmoins dire que la neutralité technologique y est directement associée dans la mesure où, par l'utilisation des termes ou par l'identification des fonctions, la Loi, sauf exception, recherche une inclusion technologique en ne favorisant pas un support ou une technologie en particulier. Certes, ce principe ne demeure pourtant pas toujours appliqué dans la mesure où certaines dispositions de la Loi ciblent une technologie en particulier. En matière de certification, par exemple, une pluralité d'articles sont venues encadrer cette technique d'identification spécifiquement[119]. Néanmoins, la Loi est construite autour de la notion de document; notion qui par essence s'applique tant à l'analogique qu'au technologique. Et, tel que nous l'avons déjà souligné, malgré son nom (qui contient le terme technologique) et malgré certaines dispositions spécifiques au technologiques[120], la LCCJTI est en bien des cas applicables à tous les supports et à toutes les technologies.

Quand avoir une loi neutre ou spécifique ? Cette manière de faire peut être associée à une méthode législative pour le moins classique (il est par exemple commun de voir l'expression « par quelque moyen que ce soit » être insérée dans les lois, comme le *Code criminel*[121], pour assurer une application inclusive de la loi qui est ainsi plus en mesure de s'adapter au temps). Cette approche peut néanmoins présenter des limites dès lors que la technologie concerne des enjeux qui ne peuvent être considérés dans un texte de portée plus générique comme la LCCJTI. On peut donc dire que la neutralité technologique prévaut par défaut et la discrimination technologique par exception.

Exemple de l'intelligence artificielle. À titre d'exemple, il existe une tendance soutenue pour que l'intelligence artificielle fasse l'objet d'un contrôle fort de la part de l'État. En premier lieu, la tendance libérale vis-à-vis de l'encadrement des technologies est critiquée et les risques potentiels

---

115 Brad A. GREENBERG, « Rethinking Technology Neutrality », (2016) 100 *Minesota Law Review* 1495, 1557.

116 *Id.*, p. 1559.

117 *Id*., p. 1559.

118 Elle n'est jamais citée dans la Loi, notamment à l'article 1 qui constitue une suite de grands objectifs à satisfaire (dont l'équivalence fonctionnelle). On peut tout de même dire que terme est utilisé pour introduire les quelques dispositions qui ont été ensuite copiées / collées dans le *Code civil du Québec*.

119 Art. 47 et ss.

120 Par exemple l'article 12 sur l'original technologique.

121 Par exemple l'article 207.1 (1) C. crim. Pour en savoir plus à ce sujet, Vincent GAUTRAIS, *Neutralité technologique : rédaction et interprétation des lois face aux changements technologiques*, Montréal, Éditions Thémis, 2012, p. 51.

associés à cette technologie[122] militent pour une reprise en main de l'appareil étatique. En second lieu, les inférences n'ont aucunement été considérées au moment de la rédaction de la Loi[123]. Or, si cette tangente devait être suivie, doit-elle s'effectuer dans le cadre d'un texte spécifique ou au contraire dans celui d'une loi et d'une structure préexistante ? Dit autrement, cette technologie pourrait-elle être envisagée par la LCCJTI ? Il est aussi envisageable de croire que le niveau de spécificité peut aussi dépendre du secteur d'activité dans lequel est développé ladite technologie[124]. À titre d'exemple, la problématique des voitures autonomes pourrait justifier un traitement spécifique par une industrie et des institutions gouvernementales dédiées, et ce, eu égard aux enjeux techniques, sociaux, sécuritaires et légaux particuliers. Notons que le choix d'opérer un traitement spécifique vis-à-vis d'un support ou d'une technologie implique un effort préalable de délimitation du champ d'application dans la mesure où les distinctions sont souvent floues entre les différents termes employés : qu'est-ce qu'une intelligence artificielle ? Est-ce que les caméras dites intelligentes en font partie ? Pour conclure sur cette question que nous évoquerons plus tard[125], il importe, au niveau de la neutralité technologique, d'envisager notamment les éléments suivants :

- la Loi est-elle substantiellement armée pour encadrer la nouveauté ?
- si non, la Loi pourrait-elle être amendée pour ce faire ?
- la technologie que l'on souhaite encadrer présente-t-elle des éléments de spécificités par rapport à d'autres supports ou d'autres technologies ?
- certaines applications plus spécifiques (par exemple les voitures autonomes; applications dans le domaine de la santé; applications relatives à la sécurité publique, utilisation dans le domaine de l'éducation[126], etc.) pourraient-elles justifier un encadrement spécifique[127] ?

PROPOSITION #3 : La notion de neutralité technologique correspond à un principe rédactionnel somme toute assez classique et généralement reconnu. Son application est à favoriser sous réserve de spécificités liées à un secteur d'activité ou à la technologie elle-même. Si tel est le cas, un traitement spécifique doit être justifié.

---

122 *Supra*, Section 1.1.

123 *Supra*, Section 1.2.2.2.1.

124 L'Angleterre a en effet opté pour le moment pour une approche plutôt sectorielle; cette position est relativement différente de l'Europe qui, en matière d'intelligence artificielle, a plutôt choisi une approche plus horizontale en ciblant plus généralement les industries à haut risque. Jaspreet TAKHAR, « UK vs Europe approach to Regulating AI: from One Extreme to Another ? », 5 avril 2023, en ligne : <https://www.connectontech.com/uk-vs-eu-approach-to-regulating-ai-from-one-extreme-to-another/>.

125 *Infra*, Section 2.1.1.1.

126 On peut notamment penser à l'appel à un traitement spécifique de la part de l'UNESCO, *Guidance for Generative IA in Education and Research*, 7 septembre 2023, en ligne : <https://unesdoc.unesco.org/ark:/48223/pf0000386693> où la proposition d'un traitement spécifique s'entend sur la double base d'une forme particulière d'intelligence artificielle (dite générative) et dans le domaine particulier de l'éducation.

127 Cette question centrale où il s'agit de considérer le traitement juridique d'une technologie plus généralement ou, au contraire de façon plus spécifique, est envisagée dans Céline CASTETS-RENARD et Jessica EYNARD, « Introduction », dans Céline CASTETS-RENARD et Jessica EYNARD (dir.), *Un droit de l'intelligence artificielle : entre règles sectorielles et régime général*. Perspectives comparées, Bruylant, Bruxelles, 2022, pp. 32-33.

PROPOSITION #4 : Le choix d'une approche technologiquement spécifique doit, d'une part, être justifié et, d'autre part, être basé sur une définition précise qui permet aisément de déterminer le champ d'application.

PARTIE 2 – LCCJTI+ : MATIÈRES À CONSIDÉRER

2.1 LCCJTI + normativité

2.1.1 État des tendances

Plan. Du fait de la densification préalablement envisagée (Section 1.2.1), on s'interroge sur les volontés différentes des gouvernements à encadrer les nouvelles situations technologiques. Aussi, plusieurs avenues se présentent sur la manière de traduire concrètement cette réappropriation du monde technique. Plusieurs tendances semblent de mise; tendances qui parfois vont se matérialiser vis-à-vis d'une technologie en particulier (comme l'intelligence artificielle) et d'autres de manière plus générale[128]. Au regard du survol mondial demandé, cinq tendances semblent pouvoir être identifiées. Les trois premières portent sur la raison d'être de la régulation où une densification du contrôle est généralement préconisée (plus d'intervention; plus de structure; plus de prescription). Les deux dernières font quant à elles état de manières de faire qui sont un peu différentes. À cet égard, nous souhaitons illustrer certains éléments de particularisme identifié.

2.1.1.1 Tendances vers une augmentation du contrôle

2.1.1.1.1 Tendances plus directives

LCCJTI: une loi en dormance. De façon étonnamment moderne, la LCCJTI avait bien évalué que le domaine du technologique étant mouvant et changeant, il importait de le « mettre à jour » en instituant une réglementation dynamique. Aussi, la loi de 2001 avait donné un vrai pouvoir d'intervention du Comité d'harmonisation[129] ainsi qu'une capacité de complétude du droit par le biais de décrets[130] ou de règlements[131]. Relativement au premier, quelques rencontres furent organisées qui ne donnèrent lieu à aucun résultat. Quant aux seconds, rien ne fut adopté. Cette inaction peut sembler étonnante. Étonnante par le fait qu'il est actuellement difficile pour les acteurs de connaitre les règles du jeu, et ce, même sur des questions plus traditionnelles comme l'intégrité documentaire, l'identité, etc. Étonnante, car même sur ces questions plutôt « anciennes », une quête de complétude réglementaire semble recherchée par la communauté[132].

Tendance interventionniste généralisée. Bien que nous ayons déjà mentionné l'opposition marquée entre Europe et Amérique du Nord[133], nous croyons néanmoins percevoir des tendances

---

128 *Supra*, Section 1.2.3.2.

129 Art. 63 et ss. LCCJTI.

130 Art. 8 LCCJTI.

131 Art. 69 et ss. LCCJTI.

132 Lors d'une étude précédente pour le ministère de la Justice en 2020, nous avions effectué un sondage auprès de plus de 80 intervenants de la communauté principalement juridique et une tendance marquée considérait le besoin de mieux identifier les règles applicables en la matière, notamment par le biais de règlements. Voir Vincent GAUTRAIS, *Étude juridique sur la Loi concernant le cadre juridique des technologies de l'information* (RLRQ c C-1.1) – Mandat du ministère de la Justice du Québec, 31 juillet 2020, p. 23 (et notamment relativement aux questions 26, 27, 32 et 34).

133 *Supra*, Section 1.2.1.2.

assez généralisées vers plus d'encadrement. Et si des différences sensibles apparaissent sur les moyens à mettre en place (de la co-régulation à l'auto-régulation), une quête vers plus de structuration réglementaire semble de mise. C'est notamment vrai dans chacun des domaines d'intervention qui suivront les présents développements sur la normativité (responsabilité, identité, sécurité). C'est également vrai pour certains questionnements plus technologiquement centrés.

Approche sectorielle. Le cas de l'intelligence artificielle. Quant à des sujets plus « à la mode », il est intéressant de constater que certaines thématiques mobilisent une réaction particulièrement active de la part des gouvernements. L'intelligence artificielle, du fait des enjeux qu'elle représente, a légitimement suscité différentes formes de réactions. La professeure Scassa a notamment remarqué que, si le projet de loi fédéral C-27 a opté pour une approche spécifique avec des instances dédiées à cette technique à contrôler, les Britanniques ont plutôt suivi de demander aux instances existantes – telles que l'ICO et autres institutions – de traiter de ces questions nouvelles[134]. L'Union européenne, à la différence de l'Angleterre, a quant à elle aussi décidé d'introduire de nouvelles instances de contrôle[135]. En d'autres mots, il s'agit soit de traiter en centrant sur l'objet d'analyse soit au contraire sur l'institution en charge de le contrôler. Substance versus institutions.

> « There is a certain attractiveness in the idea of a regulatory approach like that proposed by the UK – one that begins with existing regulators being both specifically directed and further enabled to address AI regulation within their areas of responsibility. As noted earlier, it seems far more agile than Canada's rather clunky bill. »[136]

Cette approche a bien des égards est jugée comme étant plus « neutre » et s'apparente à celle récemment choisie en matière de protection des renseignements personnels au Québec où la densification des règles qui est apparue en 2021 s'est effectuée sans modifier la structure des lois existantes et en gardant les instances en cause.

« Comité d'harmonisation 2.0 ». Le comité d'harmonisation, comme mentionné, n'a pas joué à ce jour un rôle très actif. Il faut néanmoins mentionner qu'en 2021 la Loi a été modifié par le Projet de loi 6 afin d'étendre quelque peu son rôle, les articles 63, 64 et 68 parlant désormais « d'utilisation des technologies »[137]. Au-delà de la composition dudit comité, ce changement

---

134 Teresa Scassa, en ligne : <http://www.teresascassa.ca/index.php?option=com_k2&view=item&id=370:comparing-the-uks-proposal-for-ai-governance-to-canadas-ai-bill&Itemid=80E> : « Existing regulators will be encouraged and, if necessary, specifically empowered, to regulate AI according to these principles within their spheres of regulatory authority. Examples of regulators who will be engaged in this framework include the Information Commissioner's Office, regulators for human rights, consumer protection, health care products and medical devices, and competition law ».

135 Voir le *Règlement européen sur l'intelligence artificielle*. Voir aussi Jaspreet TAKHAR, « UK vs Europe Approach to Regulating AI : From One Extreme to Another ? », 5 avril 2023, en ligne : <https://www.connectontech.com/uk-vs-eu-approach-to-regulating-ai-from-one-extreme-to-another/:>, « By contrast, the EU approach will rely on a co-ordinated network of new and established regulators, including a central European AI Board and national competent authorities for AI in each Member State ».

136 *Id.*

137 Projet de loi nº 6 (2021, chapitre 33) *Loi édictant la Loi sur le ministère de la cybersécurité et du numérique et modifiant d'autres dispositions*, sanctionné le 3 décembre 2021, en ligne : <https://www.publicationsduquebec.gouv.qc.ca/fileadmin/Fichiers_client/lois_et_reglements/LoisAnnuelles/fr/2021/2021C33F.PDF>.

législatif a aussi étendu la capacité de produire des guides, mais aussi tout « autre document »[138]. Même le titre de la Section 1 du Chapitre 4 a été étendu[139]. Cette extension du rôle du Comité n'est pas anodine et rien n'indique donc que les sujets du jour (intelligence artificielle; chaînes de blocs, etc.) ne puissent être considérés par celui-ci. Sur sa fonction essentielle, malgré cette adaptation législative de 2021, la Loi conserve son rôle « d'harmonisation ». Il est vrai que ce Projet de loi 6 instituant la *Loi sur le ministère de la Cybersécurité et du Numérique* est aussi à l'origine d'un autre comité (art. 9) dont il n'est pas tout à fait clair en quoi il se distancie de celui lié à la LCCJTI.

Au-delà de l'harmonisation. Le terme est générique; vague. Il représente le vœu emprunt dans ce texte de ne pas s'isoler du monde. Il est moins parlant sur ce que le Comité peut faire. Là encore, néanmoins, il semble qu'une vision extensive du rôle du Comité peut être envisagée. Dans un premier temps, il ne doit pas se limiter à un seul rôle de production normative. Certes, dans sa version originale, la Loi privilégiait celui-ci. D'ailleurs, à cet égard, le BNQ, dont le rôle premier est de « produire » des normes, présidait ledit Comité. Dans un deuxième temps, nous croyons que le texte en l'état valorise une approche extensive également relativement aux rôles possibles. Aussi, il pourrait très bien jouer un rôle d'identification des besoins des acteurs du domaine; une identification des textes qui pourraient servir de modèle; plus généralement, un rôle d'animation normative[140].

Nouveaux rôles. Plusieurs fonctions de ce comité réinventé pourraient être ajoutées. Nous nous autorisons à identifier certaines d'entre elles. En premier lieu, au-delà des seuls standards, le Comité est pleinement habilité à travailler sur des standards, des guides, mais également « tout autre document », ce qui laisse supposer que cela pourrait concerner des exemples de contrats de politiques internes, de lignes directrices, etc. Une liberté d'action qui semble en l'occurrence salutaire... En effet, de façon presque systématique, les lois réfèrent à des standards ou autres normes informelles qui elles-mêmes réfèrent à des politiques internes que les acteurs (publics ou privés) doivent produire. De façon presque systématique donc, on aperçoit ce « mille-feuilles normatif » auquel nous avons déjà référé, impliquant minimalement 1) normes formelles (lois, règlements; décrets); 2) normes informelles (lignes directrices, guides, certification, etc.); 3) normes individuelles (politiques, mesures, EFVP, documentations internes, etc.). Or, actuellement, beaucoup de ces acteurs sont assez démunis pour ce faire. Par animation normative, ledit comité pourrait donc participer ou favoriser l'adoption de modèles. À titre de comparaison, dans le domaine plus fraichement régulé de la protection des renseignements personnels, on

---

138 Voir notamment les articles 65, 66 et 67 LCCJTI.

139 On est passé de « Normes et standards techniques » à « Normes, des standards et autres éléments visant l'utilisation des technologies ».

140 Vincent GAUTRAIS, *Étude juridique sur la Loi concernant le cadre juridique des technologies de l'information* (RLRQ c C-1.1) – Mandat du ministère de la Justice du Québec, 31 juillet 2020, pp. 22, 26, 80. Voir aussi la recommandation 24, page 81.

aperçoit ce type d'animation tant au niveau informel[141] qu'individuel[142]. On aperçoit ce même travail de coordination dans le cadre du DSA où un comité dédié tente de remplir ce rôle dans le cadre de la fédération européenne, et ce, selon des fonctions proches de ce que nous dénommons « animation normative »[143]. En deuxième lieu, le comité dit d'harmonisation pourrait également, comme mentionné précédemment, jouer un rôle de dialogue interinstitutionnel[144]. Il nous semble en effet que la transversalité de certaines technologies, comme l'intelligence artificielle, nous invite à unifier les ressources susceptibles d'être affectées par le numérique. Comme dans l'exemple britannique précité, une coordination des perspectives s'impose et il est facile d'identifier des instances qui devraient unir leurs efforts. Cette collaboration concerne les instances dédiées à la protection d'un intérêt catégoriel précis (citoyen (*Commission des droits de la personne*), individu (*Commission d'accès à l'information*), consommateur (*Office de protection du consommateur*), etc.) ou à un secteur d'activité donné (automobile, éducation, santé)). En troisième lieu, et du fait de la généralité associée au comité d'harmonisation, ce dernier pourrait avoir un rôle pour déterminer si une question mérite d'être considérée de façon plus « neutre » ou, au contraire, de façon plus spécifique. Dit autrement, en reprenant nos développements sur la neutralité technologique[145], le comité pourrait jouer le rôle de détermination si une question donnée mérite d'être considérée de façon générale ou, au contraire, par le spectre d'un secteur d'activité spécifique.

PROPOSITION #5 : Même si sa structuration n'a pas besoin de se comparer aux exemples européens, nous croyons que l'avènement de débats sociétaux importants en lien avec certaines évolutions technologiques pourrait être l'occasion de revigorer le rôle du Comité d'harmonisation, et ce, en conformité avec quelques amendements législatifs récents (2021) qui semblent offrir une plus grande liberté d'action audit comité.

---

141 Avec la Loi 25, la Commission d'accès à l'information dispose de la possibilité accrue de présenter des lignes directrices (art. 45). La situation est similaire avec le RGPD (art. 70 d)). On trouve également ce type de normes dans le domaine financier où l'OSFI (Office of the Superintendent of Financial Institutions) a élaboré des Lignes de conduite en matière de « regtechs » (*infra*, Section 2.1.1.2.2.2), particulièrement dans la relation contractuelle entre la banque et la compagnie tierce qui effectue les rapports de conformité (compliance). (Guidelines B-10).

142 Modèle d'EFVP de la Commission d'accès à l'information. Voir notamment la nouvelle mouture du 22 septembre 2023.

143 Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE, On peut notamment lire à l'article 63 s'intitulant « Missions du comité » : « 1. Lorsque cela est nécessaire pour réaliser les objectifs énoncés à l'article 61, paragraphe 2, le comité : a) soutient la coordination d'enquêtes conjointes; b) soutient les autorités compétentes dans l'analyse des rapports et résultats des audits réalisés auprès des très grandes plateformes en ligne ou des très grands moteurs de recherche en ligne dont le présent règlement prévoit la transmission; c) émet des avis, des recommandations ou des conseils destinés aux coordinateurs pour les services numériques conformément au présent règlement, en tenant compte notamment de la liberté des fournisseurs de services intermédiaires de fournir des services; d) conseille la Commission en ce qui concerne les mesures visées à l'article 66 et adopte des avis concernant les très grandes plateformes en ligne ou les très grands moteurs de recherche en ligne conformément au présent règlement; e) soutient et encourage l'élaboration et la mise en œuvre de normes européennes, lignes directrices, rapports, modèles et codes de conduite, en collaboration avec les parties prenantes pertinentes, comme le prévoit le présent règlement, y compris en émettant des avis ou des recommandations sur les questions liées à l'article 44, ainsi que l'identification des questions émergentes, en ce qui concerne les matières relevant du présent règlement. » (Notre soulignement)

144 *Infra*, Section 2.1.1.1.2.

145 *Supra*, Section 1.2.3.2.

Le rôle du comité devrait être revu, au-delà de la seule harmonisation initialement prévue et s'étendre à un rôle plus large d'animation normative. Son rôle devra aussi être envisagé de concert avec celui qui prévaut dans la *Loi sur le ministère de la Cybersécurité et du Numérique.*

2.1.1.1.2 Tendances plus structurantes

Plus de structure. Au regard des textes étudiés, nous apercevons un éclatement des approches qui se diversifient tant par les types d'acteurs (privés, gouvernementaux, publics, société civile), de disciplines (entre droit, gestion et technologie) que par les types de règles (lois, règlements, lignes directrices, modèles, etc.). Aussi, pour contrer cette complexité déjà considérée[146], il importe de pallier cet état de fait par une structuration du traitement de ces enjeux. Cette dernière est susceptible de se matérialiser de différente manière.

Plus de dialogue internormatif. Il importe d'intégrer cette nouvelle réalité selon laquelle un « mille-feuilles normatif » est désormais de mise pour réguler les technologies. Or, si classiquement les lois réfèrent à des lignes directrices[147], codes de conduite[148], standards, règles de l'industrie[149], il faut aussi agir au niveau documentaire. Ce besoin se fait particulièrement sentir pour les petites et moyennes entreprises qui sont souvent démunies, ne disposant pas toujours des ressources nécessaires, alors que la prise en compte de leurs intérêts est pourtant souvent identifiée[150].

Structuration institutionnelle. Classiquement, un texte de loi peut bénéficier d'une structure administrative qui vient consolider son application. Si cela vaut pour tous les domaines du droit, cela vaut peut-être encore plus dans le domaine du numérique dès lors que les enjeux sociétaux sont d'importance et que les manières d'y parvenir sont à la fois complexes et incertaines. Après, notre survol en droit comparé du numérique nous oblige à rappeler les différences culturelles qui prévalent notamment entre l'Europe et l'Amérique[151]. À titre d'exemple, la récente mouture du projet de Règlement européen sur l'intelligence artificielle traduit la présence d'instances tant au niveau de la Commission que des États membres[152]. Il en est de même au regard du Règlement eIDAS sur l'identité numérique où, notamment, les différents agréments ou autres accréditations permettent de déduire des présomptions quant à la qualité des signatures ou autres services de

---

146 *Supra*, Section 1.2.2.1.

147 Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, LQ 2021, c. 25, article 45.

148 RGPD (art. 40), DMA, DSA, etc.

149 *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, LQ 2021, c. 25, art. 28 et 119 : « Les renseignements anonymisés en vertu de la présente loi doivent l'être selon les meilleures pratiques généralement reconnues et selon les critères et modalités déterminés par règlement ».

150 Voir notamment le RGPD (art. 40 et aussi les considérants 13, 98, 132, 167). Voir aussi les traités précités comme ACEUM (art. 19.17.1), le traité entre le Chili, Singapour et la Nouvelle-Zélande et le *Free Trade Agreement* entre le United Kingdom of Great Britain, Northern Ireland et la Nouvelle-Zélande.

151 *Supra*, Section 1.2.2.3.1.

152 Projet de Règlement européen sur l'intelligence artificielle, version du 09 juin 2023, notamment les art. 30 et ss.

confiance[153]. Plus généralement, cette structuration institutionnelle semble le gage d'un plus grand contrôle des manières de faire.

> « Institutional and legal structures are important factors shaping the possibilities and practical dimensions of the implementation of algorithmic accountability policies. Enabling legal frameworks can provide important incentives to operationalise algorithmic accountability policies within public agencies that use algorithmic systems. »[154]

Structuration financière. Le niveau de structuration institutionnelle va également dépendre du support financier qui est octroyé à une instance. L'information n'est pas toujours facile à trouver, surtout dans les pays étrangers. En revanche, il est un peu plus simple de connaître les sommes allouées au Canada. À titre d'exemple, la hausse de moyens financiers dont la Commission d'accès à l'information se traduit dans un budget qui a été presque doublé de 2016/2017 à 2023/2024[155]. Il en va de même au Canada pour le Commissariat fédéral de protection de la vie privée (CPVP)[156]. Comme mentionné dans le paragraphe précédent, cette augmentation se justifie tant en raison des enjeux sociétaux qu'aux caractères complexes et incertains du domaine de la protection des renseignements personnels. Également, il importe de citer les sommes importantes qui ont été allouées au Conseil canadien des normes dans le domaine de l'intelligence artificielle, mais plus généralement de la gouvernance des données.

> « Following the publication of the 2021 Canadian Data Governance Standardization Collaborative Roadmap (DGSC Roadmap), and in support of the Pan-Canadian Artificial Intelligence Strategy (PCAIS) and the forthcoming implementation of the Artificial Intelligence and Data Act (AIDA), as part of the Digital Charter Implementation Act, 2022, the Standards Council of Canada (SCC) received a combined $17M and $2.3M ongoing under Budget 2021 to advance standardization strategies for both Artificial Intelligence (AI) and Data Governance. »[157]

Structuration inter-institutionnelle. Dans le contexte européen de la régulation du numérique, nous constatons le besoin de créer plus qu'un dialogue institutionnel, mais une véritable

---

153 Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE et notamment tout ce qui touche aux services d'identité et de confiance faisant l'objet d'une qualification. La distinction entre les services de signature ou de confiance qui sont accrédités et ceux qui ne le sont pas donne lieu à l'émergence d'une pareille présomption dans la Loi-modèle de la CNUDCI récemment adoptée en 2022 (art. 23 et 24).

154 ADA LOVELACE INSTITUTE, *AI Now Institute and Open Government Partnership, Algorithmic accountability in the public sector - Executive summary*, 2021, p. 10, en ligne : <https://ainowinstitute.org/publication/algorithmic-accountability-for-the-public-sector-report>.

155 GOUVERNEMENT DU QUÉBEC, Budget de dépenses 2023|2024, vol. 3, p. 139, en ligne : <https://www.tresor.gouv.qc.ca/fileadmin/PDF/budget_depenses/23-24/3_Credits_depenses_portefeuilles.pdf> où le budget de la CAI est désormais à 12 594 millions de dollars alors qu'il était à 8 165 l'année précédente.

156 Voir notamment la Comité permanent de l'industrie et des technologies, 26 septembre 2023, en ligne : <https://parlvu.parl.gc.ca/Harmony/fr/PowerBrowser/PowerBrowserV2/20230926/-1/39921> où le ministre Champagne évoque une hausse de 20 millions pour cette institution en 2023.

157 CONSEIL CANADIEN DES NORMES, Backgrounder : Launching of the AI and Data Governance Standard Collaborative, 11 juillet 2023 (Document de travail).

collaboration entre la multitude des instances en charge de traiter du numérique. **En premier lieu**, ce besoin se situe institutionnellement dans le fait que l'uniformisation est une composante centrale de la construction européenne; on souhaite avoir un même droit dans l'ensemble des 27 pays membres. **En deuxième lieu**, cette collaboration se justifie substantiellement car il est de plus en plus difficile de cloisonner le numérique qui est transversal par essence. Ainsi, la Loi va selon les cas toucher une même personne avec un statut distinct. Ainsi, à titre d'exemple, l'usage d'une plateforme par une personne individuelle pourra la concerner comme citoyen (en lien avec les libertés fondamentales, comme individu (concernant la vie privée), comme consommateur (concernant l'application de la *Loi sur la protection du consommateur*), etc. À titre d'illustration, le *Projet de loi français visant à sécuriser et réguler l'espace numérique*[158] traite des mineurs (art. 2), des citoyens (art. 4A), des joueurs (art. 15), des consommateurs (art. 26), etc. À cet égard, le DSA européen (*Digital Services Act*) prend le soin d'identifier une institution auprès de chaque État membre « comme leur coordinateur pour les services numériques »[159]. **En troisième lieu**, cette structuration entre les institutions peut se justifier tout simplement pour des fins de rationalisation des ressources. Des auteurs, économistes, sont en effet suspicieux quant à la capacité fonctionnelle de la Commission européenne de parvenir à imposer l'application du DSA et du DMA à des entreprises mondiales (notamment les GAFAM) disposant de ressources incroyablement importantes[160]. Ainsi, la Commission européenne doit coopérer avec les instances nationales tout bonnement pour augmenter sa « force de frappe » contre une industrie toute puissante. On peut même lire dans le DSA que cette coopération est requise si l'on veut créer a « common union supervisory capacity »[161]. Sans forcément se limiter à ce rapport de force, il s'agit simplement de mutualiser ses ressources dans un domaine qui requiert une expertise exigée par la complexité précitée. Cela dit, si elle se traduit formellement dans les textes en Europe, le besoin se fait également sentir de l'autre côté de l'Atlantique, surtout dans un contexte fédéral[162]. Notons que cette approche correspond à certains égards à ce que l'on nomme au Canada du « fédéralisme collaboratif » et qui se traduit notamment en matière de renseignements personnels où différentes instances compétentes unissent leurs forces pour répondre à des initiatives internationales, sources de menaces, comme notamment relativement à l'affaire *Clairview AI*[163].

---

158 Projet de loi français du 5 juillet 2023 visant à sécuriser et réguler l'espace numérique, en ligne : <www.senat.fr/leg/tas22-156.html>.

159 Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE, article 49.

160 Jean CATTAN et Joëlle TOLEDANO, « La Commission dans la mise en œuvre du DMA : citadelle assiégée ou chef d'orchestre ? », *Concurrences*, n° 3, 2022, p. 3.

161 DSA, considérant 137.

162 TREASURY BOARD OF CANADA SECRETARIAT, Government of Canada, Algorithmic Impact Assessment Tool, 2019, en ligne : < https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html>. Voir aussi ADA LOVELACE INSTITUTE, *AI Now Institute and Open Government Partnership, Algorithmic Accountability in the Public Sector - Executive Summary*, 2021, p. 16, en ligne : <https://ainowinstitute.org/publication/algorithmic-accountability-for-the-public-sector-report>.

163 Enquête conjointe sur Clearview AI, Inc. par le Commissariat à la protection de la vie privée du Canada, la Commission d'accès à l'information du Québec, le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique et le Commissariat à l'information et à la protection de la vie privée de l'Alberta, *Conclusions en vertu de la LPRPDE no 2021-001*, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2021/lprpde-2021-001/>.

PROPOSITION #6 : En tenant compte de la moindre structuration institutionnelle qui prévaut en Amérique du Nord, en général, et au Québec, en particulier, il est néanmoins possible de croire que le Comité d'harmonisation pourrait jouer un rôle de coordination / animation, et ce, tant au niveau substantiel, entre les instances provinciales, qu'au niveau fédéral. Celui-ci devrait pouvoir disposer de moyens pour ce faire, et ce, en fonction du rôle d'animation précité. Ce rôle d'animation devrait notamment pouvoir se matérialiser par l'identification ou la production de modèles de politiques internes rendus disponibles auprès des acteurs, notamment les petites et moyennes entreprises. Le droit applicable doit donc être envisagé dans le cadre de rapport internormatif entre les lois, les normes informelles et les documentations internes.

2.1.1.1.3 Tendances plus prescriptives

2.1.1.1.3.1 Plus de prescription sur le fond

Densification des règles généralisée. Nous le verrons dans les sections suivantes, la généralisation de l'utilisation du numérique entraîne une hausse sensible des obligations des acteurs. Du fait de la hausse des risques individuels et sociaux[164] et de la hausse du contrôle de certains acteurs sur les données, des règles récentes viennent densifier les obligations concernant la responsabilité[165], l'identité[166] et la sécurité[167]. À certains égards, la grande généralité associée à la LCCJTI de 2001, si elle correspondait aux manières de faire de l'époque, a quelque peu vécu.

2.1.1.1.3.2 Plus de prescription sur la sanction

Sanctions augmentées. Cette tendance prescriptive se trouve aussi dans le fait que plusieurs des lois en lien avec l'encadrement du numérique prennent le soin d'associer le non-respect de celles-ci par des sanctions qui peuvent être conséquentes. Évidemment, le modèle vient de l'Europe où le RGPD est sans doute l'illustration la plus significative. En effet, le 4 ou 5 % du chiffre d'affaires de l'entreprise concernée frappe les esprits[168]; et les portefeuilles. La solution est d'ailleurs très similaire avec le nouveau règlement européen sur l'intelligence artificielle où la sanction peut même aller jusqu'à 6 %[169] tout comme les fameux DMA[170] et DSA. Dans un autre texte en cours d'étude, le projet de loi français de juillet 2023 visant à sécuriser et réguler l'espace numérique[171] évoque des sanctions similaires de 1 à 6 % du chiffre d'affaires mondial de l'entreprise, et ce, pour

---

164 *Supra*, Section 1.1.1.2.

165 *Infra*, Section 2.2.

166 *Infra*, Section 2.3.

167 *Infra*, Section 2.4.

168 RGPD, art. 83 (4), (5) et (6).

169 Article 71 (3) du Règlement établissant des règles harmonisées concernant l'intelligence artificielle.

170 Une annonce en septembre 2023 sur les 6 contrôleurs d'accès identifiés par la Commission européenne (Alphabet, Amazon, Apple, Bytedance, Meta Microsoft) sur la base du DMA obligent ces derniers à respecter un certain nombre d'obligations qui, en cas de non-respect, peut aller jusqu'à 10 voire 20 % du chiffre d'affaires mondial. Pour en savoir plus, consulter <https://ec.europa.eu/commission/presscorner/detail/fr/ip_23_4328>.

171 Projet de loi français du 5 juillet 2023 visant à sécuriser et réguler l'espace numérique, en ligne : <www.senat.fr/leg/tas22-156.html>. Voir notamment l'article 2 ajoutant une disposition après l'article 10 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

des infractions en lien avec la protection des mineurs (art. 2), des citoyens (art. 4), des consommateurs (art. 2 bis), etc.

Influence externe. De façon étonnamment comparable[172], la solution de la « peur du gendarme » a été suivie au Québec (Loi 25[173]) mais aussi par le Canada avec le C-27[174]. Dans ce dernier cas, il est tout de même symptomatique d'une certaine différence « culturelle » dans la mesure où le législateur prend le soin de mentionner que : « **95 (6)** L'infliction de la pénalité vise non pas à punir mais à favoriser le respect de la présente loi ».

On peut aussi rapidement citer la situation de la Chine qui adopta un texte venant « calquer » la situation européenne en matière de protection des renseignements personnels vis-à-vis des entreprises du secteur privé. Le *Personal Information Protection Law* (PIPL) prévoit en effet à son article 62 que :

> « Where the circumstances of the unlawful acts mentioned in the preceding Paragraph are grave, the departments fulfilling personal information protection duties and responsibilities order correction, confiscate unlawful income, and impose a fine of not more than 50 million Yuan, or 5 % of annual revenue. »[175]

Résistance. Aux États-Unis, la donne est sensiblement différente. En matière d'intelligence artificielle, le débat tourne pour le moment uniquement sur un cadre « volontaire »[176] et donc, forcément, dénué de sanction. Pour le moment, l'Angleterre n'a pas non plus introduit de sanction additionnelle[177].

---

172 Étonnamment car si l'Europe et son marché de plus de 400 millions de consommateurs est sans doute capable de sanctionner des multinationales avec de tels pourcentages de punition, il est possible de croire que la capacité de sanctions si énormes pourrait être sensiblement plus difficile à appliquer par une instance du Québec ou du Canada.

173 La *Loi sur la protection des renseignements personnels dans le secteur privé* (RLRQ c P-39.1) a été modifiée par la Loi 25 aux articles 90.12 et 91, afin d'établir désormais une sanction pouvant aller à soit 2 ou 4 % « du chiffre d'affaires mondial de l'exercice financier précédent ».

174 Projet de loi C-27 : Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois, juin 2022, art. 95 (4) et 128 pour les questions de protection de renseignements personnels. Pour les problématiques touchant à l'intelligence artificielle, voir les art. 30(3) et 40. Dans C-27, les pourcentages sont de 2 à 5 % « des recettes globales brutes de la personne au cours de son exercice précédant celui pendant lequel elle a été condamnée ».

175 Une version en anglais est disponible en ligne : <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-draft-personal-information-protection-law-full-translation/>. Si l'on retrouve la mention du 5 % du revenu annuel de l'entreprise, la référence aux 50 millions de yuans est l'équivalent de moins de 10 millions de dollars canadiens.

176 The White House. FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI, juillet 2023, en ligne : <https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/>.

177 Jaspreet TAKHAR, « UK vs Europe Approach to Regulating AI : From One Extreme to Another ? », avril 2023, en ligne : <https://www.connectontech.com/uk-vs-eu-approach-to-regulating-ai-from-one-extreme-to-another/>.

2.1.1.2 Tendances quant aux manières de réguler le technologique

2.1.1.2.1 Tendances participatives

2.1.1.2.1.1 Intérêts véritables d'une telle approche

Participation et gouvernance. Il est étonnant de constater comment, depuis quelques années, un véritable engouement est perceptible vis-à-vis de l'approche participative. Au-delà d'une tendance à apercevoir « la promotion de la pluralisation des formes d'expression de la volonté générale »[178], il est difficile de clairement comprendre ce phénomène. **Dans un premier temps**, cette participation passe par une double délégation qui s'opère de la part des lois vers des normes techniques et des normes techniques vers des normes individuelles édictées par les acteurs eux-mêmes. La construction normative autour du technologique implique donc la communauté au regard de ces deux dernières strates.

> « As a result, the administrative state is now more of a co-equal in crafting regulations for emerging technologies and innovations requiring more consent from industry and civil society to effectively regulate these new industries. Scholars often refer to the need for new forms of "governance ... that move beyond traditional command-and-control policymaking and enforcement to improve the effectiveness and legitimacy of regulation". Another common term for this is "co-regulation", a form of governance driven by the "hope that active engagement with industry partners will make the resulting requirements more feasible and more widely accepted by regulated parties." In this new governance space, soft law mechanisms are increasingly becoming the primary means by which federal agencies craft rules and regulations governing new emerging technologies. »[179]

À titre d'exemple, c'est exactement ce qui s'opère dans la Loi 25 quand vient le temps d'anonymiser des données : l'article 23 de la *Loi sur la protection des renseignements personnels dans le secteur privé* réfère aux « meilleures pratiques de l'industrie » qui elles-mêmes exigent l'élaboration de documentations internes. En lisant les débats parlementaires relatifs à la Loi 25, on se rend compte que la volonté de plusieurs parlementaires était d'insuffler ainsi une flexibilité tout en reconnaissant la nécessité de « guides » et de « lignes directrices » pour opérer ce type d'opération[180].

Participation et élaboration des règles. La participation s'entend aussi, **dans un deuxième temps**, dans la possibilité de voir une grande variété d'acteurs, et notamment les citoyens, à participer à

---

178 Éric BUGE, « Les citoyens peuvent-ils participer à l'expression de la volonté générale en régime représentatif ? », dans Mathilde HEITZMANN-PATIN et Julien PADOVANI (dir.), *La participation du citoyen à la confection de la loi*, Mare & Martin, Paris, 2021, p. 70.

179 Ryan HAGEMANN, Jennifer HUDDLESTON SKEES and Adam THIERER, « Soft Law for Hard Problems : The Governance of Emerging Technologies in an Uncertain Future », (2018) 17-1 *Colorado Technology* LJ 37.

180 Vincent GAUTRAIS et Henry LAVILLE, « Plaidoyer pour une gouvernance participative des données personnelles au Québec », dans Cyril SINTEZ (dir.), *Mélanges en l'honneur de Catherine Thibierge*, Mare et Martin, Paris, 2023, p. 199, à la page 206.

l'élaboration des règles. Ainsi, dans une optique de meilleure représentativité, on s'assure que le plus grand nombre puisse intervenir bien au-delà de l'espace parlementaire habituel[181].

Participation et partage du contrôle. Une autre manière de comprendre la participation peut aussi passer, de façon plus prosaïque, en Europe, par un appel à la convergence des ressources. **Dans un troisième temps** donc, du fait d'un manque de moyen des instances publiques à contrôler certaines industries, notamment les plus puissantes, de plus en plus d'interprètes croient qu'il faut unir les instances publiques afin d'assurer un meilleur contrôle des activités industrielles : « L'idée selon laquelle la mise en œuvre effective du DSA en particulier vis-à-vis des réseaux sociaux requerra la participation multiforme de la société commence à être partagée »[182].

Appel à la participation dans les textes. De nombreux textes envisagent la participation sous l'une de ces formes précitées; notamment la deuxième. **En premier lieu**, les textes éthiques ont largement véhiculé cette idée sous des termes de co-construction, d'approche « bottom-up »[183] ou, plus généralement, de participation. La *Déclaration de Montréal*, par exemple en matière d'intelligence artificielle, a non seulement développé l'idée mais l'a mis en pratique[184]. **En deuxième lieu**, une telle perspective est également de mise auprès de certaines instances qui cherchent à confectionner de l'adhésion de la part de la communauté. On pense notamment au Conseil canadien des normes qui, fort d'un mandat à développer des normes en matière d'intelligence artificielle, se dote expressément de cette approche[185]. **En troisième lieu**, il est intéressant de remarquer que la participation est expressément considérée dans certains traités récents. Ainsi, on peut notamment citer le *Digital Partnership Agreement* qui fut signé le 11 juin 2020 entre le Chili, Singapour et la Nouvelle-Zélande – et pour lequel le Canada a signifié un intérêt – dont la participation constitue un leitmotiv particulièrement récurrent[186]. De façon équivalente, le *Free Trade Agreement* entre le Royaume-Uni, l'Irlande du Nord et la Nouvelle-Zélande identifie l'importance d'une prise en compte des vues diversifiées de la population civile et industrielle[187]. Une même perspective est perceptible dans le règlement européen sur la

---

181 Voir par exemple Mathilde HEITZMANN-PATIN et Julien PADOVANI (dir.), *La participation du citoyen à la confection de la loi*, Mare & Martin, Paris, 2021.

182 Joelle TOLEDANO, « La commission européenne, la norme et sa puissance », (2023) 2 *Pouvoirs* 83 à 95, en ligne : <https://www.cairn.info/revue-pouvoirs-2023-2-page-83.htm>.

183 Hannah BLOCH-WEHBA, « Algorithmic Governance from the Bottom Up », (2022) 48-1 *Brigham Young University Law Review* 69-136.

184 Marc-Antoine DILHAC, Christophe ABRASSARD et Nathalie VOARINO, *Rapport de la déclaration de Montréal pour un développement responsable de l'intelligence artificielle*, 2018, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/handle/1866/22498>.

185 CONSEIL CANADIEN DES NORMES, *Canadian Data Governance Standardization Roadmap*, 2021, en ligne : <https://www.scc.ca/en/system/files/publications/SCC_Data_Gov_Roadmap_EN.pdf>.

186 *Digital Partnership Agreemen*t, 2020, en ligne : <http://www.sice.oas.org/trade/DEPA/DEPA_Text_e.pdf>. On peut notamment lire le module 11 s'intitulant « Digital Inclusion » où l'on peut lire ceci : « The Parties acknowledge the importance of digital inclusion to ensure that all people and businesses have what they need to participate in, contribute to, and benefit from the digital economy ». Également, dans le module 10 sur les PMEs, il est noté que leur participation est particulièrement souhaitée.

187 *Free Trade Agreement between the United Kingdom of Great Britain and Northern Ireland and New Zealand*, 2022, chap. 15, en ligne : <https://www.gov.uk/government/publications/uk-new-zealand-fta-chapter-15-digital-trade>. Ce texte est très similaire au précédent.

régulation de l'intelligence artificielle[188]. Pour finir ce point, **en quatrième lieu**, paradoxalement, c'est peut-être dans les lois elles-mêmes que cet appel se fait le moins sentir. Il importe néanmoins de mentionner la *Loi française pour une République numérique* qui a donné lieu à une consultation citoyenne[189] où 21 330 citoyens ont participé.

2.1.1.2.1.2 Risques d'une participation mal contrôlée

Cette approche doit néanmoins ne pas faire oublier que plusieurs auteurs considèrent que cette ouverture vers les « parties prenantes » est parfois vue comme un prétexte pour l'État en charge de la régulation, soit d'obtenir une liberté d'action, soit d'insuffler une trop grande voix à l'industrie[190]. Shumpeter voyait déjà avec beaucoup de suspicion une telle ouverture vers une trop grande participation : « institutional arrangement for arriving at political decisions in which individuals acquire the power to decide by means of a competitive struggle for the people's vote »[191].

De tout temps, le phénomène représentatif visait à limiter l'action du citoyen « que pour choisir ses représentants »[192]. Une rupture est néanmoins intervenue avec l'article 6 de la *Déclaration des droits de l'homme* où une référence expresse est faite à l'intervention de la société civile dans la confection des normes : « tous les citoyens ont le droit de concourir personnellement ou par leurs représentants à la formation de la loi »[193].

Malgré cela, des risques sont souvent associés à de tels processus s'ils n'offrent pas des garanties suffisantes de légitimité. Aussi, deux objections majeures y sont généralement apposées : le populisme et l'ignorance[194]. Afin de tenter de les endiguer, il importe de formaliser, notamment juridiquement, une telle approche participative.

2.1.1.2.1.3 Formalisation d'une approche participative

Il importe donc de formaliser officiellement la possibilité pour certains types d'acteurs d'intervenir dans l'élaboration des règles, et ce, que ce soit pour les lois, les normes informelles ou les normes

---

188 Règlement européen sur l'intelligence artificielle où l'article 69 incite la participation de la population à l'élaboration des codes de conduite qui ne concernent pas les systèmes d'intelligence artificielle à haut risque.

189 Ministère de la transformation et de la fonction publique. La loi pour une République numérique se construit avec les Français. (mars 2019)O, en ligne : <https://www.modernisation.gouv.fr/outils-et-formations/la-loi-pour-une-republique-numerique-se-construit-avec-les-francais>.

190 Grégoire CHAMAYOU, La société ingouvernable : une généalogie du libéralisme autoritaire, Paris, La Fabrique Éditions, 2018, p. 164.

191 Cité par Hannah BLOCH-WEHBA, « Algorithmic Governance from the Bottom Up », (2022) 48-1 *Brigham Young University Law Review* 69 128-129.

192 Montesquieu, *De l'esprit des lois*, Gallimard, *La Pléiade*, Paris, p. 240.

193 Cité par Dominique ROUSSEAU, « La figure multidimensionnelle du citoyen de la démocratie continue », dans Mathilde HEITZMANN-PATIN et Julien PADOVANI (dir.), *La participation du citoyen à la confection de la loi*, Mare & Martin, Paris, 2021, p. 164.

194 Marc-Antoine DILHAC, Christophe ABRASSARD et Nathalie VOARINO, *Rapport de la déclaration de Montréal pour un développement responsable de l'intelligence artificielle*, 2018, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/handle/1866/22498>, p. 47.

individuelles. Sans prétention d'exhaustivité, nous souhaitons juste identifier certaines possibilités trouvées çà et là au gré de nos lectures.

a) Acteurs en général

Actions possibles. Face à ces appétits pour plus de participation, il importe de se demander comment elle est susceptible de se matérialiser. Nous nous plaisons à reproduire les bases méthodologiques qui ont été utilisées par la *Déclaration de Montréal pour une intelligence artificielle responsable*[195]. Dans ce texte, on préconise la mise en place de :

> « dispositifs délibératifs soulignés par Blondiaux et Sintomer dans leur article *L'impératif délibératif* : rendre possible l'imagination de solutions nouvelles dans un monde incertain; permettre une progression en généralité et viser des consensus ou des « désaccords délibératifs » dans une société marquée par le pluralisme des valeurs; et enfin, donner une source factuelle et normative de la légitimité par l'inclusion de tous à ces délibérations. »[196]

Souvent, l'approche inclusive n'est pas initiée au début du processus, mais elle intervient par la suite, les responsables prenant conscience qu'au-delà de la confection des règles, la prise en compte des populations affectées améliore la mise en application[197].

Actions variées. Une certaine variété existe quant aux manières de faire : des invitations d'experts de façons diversifiées, aux audiences publiques plus ouvertes, incluant soit des personnes affectées, soit le grand public, il importe en tout état de cause que la consultation soit suffisamment réelle pour être significative[198]. Cette prise en compte des intérêts des parties prenantes est par exemple reprise dans l'élaboration des différentes normes selon le *Digital Services Act* européen (DSA)[199].

b) Lanceurs d'alerte

Solution à améliorer. Une autre avenue qui est parfois envisagée pour densifier le contrôle des technologies est celle des lanceurs d'alerte. L'idée est simple : face au manque de transparence dont certaines entreprises témoignent, il semble pertinent de faciliter des acteurs de l'intérieur de

---

195 Pour avoir plus d'information sur cette initiative, voir en ligne : <https://declarationmontreal-iaresponsable.com/>.

196 Marc-Antoine DILHAC, Christophe ABRASSARD et Nathalie VOARINO, *Rapport de la déclaration de Montréal pour un développement responsable de l'intelligence artificielle*, 2018, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/handle/1866/22498>, p. 56. La source des auteurs cités est la suivante : Loïc BLONDIAUX et Yves SINTOMER, *L'impératif délibératif*, revue *Politix*, 2002, p. 25-26.

197 ADA LOVELACE INSTITUTE, *AI Now Institute and Open Government Partnership, Algorithmic Accountability in the Public Sector - Executive Summary*, 2021, p. 15, en ligne : <https://ainowinstitute.org/publication/algorithmic-accountability-for-the-public-sector-report>.

198 R. RICHARDSON (ed.), « Confronting Black Boxes : A Shadow Report of the New York City Automated Decision System Task Force », AI Now Institute, 2019, en ligne : <https://ainowinstitute.org/ads-shadowreport-2019.pdf>.

199 DSA, où l'article 63 prévoit que le Comité européen de service numérique « e) soutient et encourage l'élaboration et la mise en œuvre de normes européennes, lignes directrices, rapports, modèles et codes de conduite, en collaboration avec les parties prenantes pertinentes ».

« couler » des informations susceptibles d'informer le public, et les pouvoirs publics, de pratiques illégales ou non éthiques. La quête d'une telle protection est d'autant plus justifiée que nous sommes avec le numérique dans un domaine opaque, complexe, changeant. Si les exemples de cadres législatifs sont assez nombreux, même au Canada[200] et au Québec[201], il semble que certains problèmes prévalent :

- ne fonctionne pas toujours si divulgation directement au grand public[202];
- distorsion selon les statuts privé ou public des lanceurs d'alerte;
- problème de détermination du domaine d'application (définition changeant de ce qu'est un lanceur d'alerte);
- compatibilité avec les règles prévalant en protection des renseignements personnels; etc.

Solution plébiscitée. Au regard d'un cadre légal sans doute plus robuste, l'Europe joue encore sur ce point un rôle de meneur[203], la mise en place d'un processus de lanceur d'alerte étant même parfois obligatoire auprès de certaines entreprises[204]. Plusieurs projets de lois apparaissent « dopés » par l'opacité accrue dans le domaine du numérique[205] ou la toute-puissance de l'industrie[206]. Ce statut accentue le « métier de citoyen »[207] et est donc souvent vu comme un moyen permettant à la fois d'accentuer l'implication des individus tout en ajoutant un moyen d'action dans un domaine qui en a bien besoin. Des acteurs de ce domaine du numérique, et notamment de la sécurité, qui prétendent parfois que l'absence d'un cadre de protection adéquat pour les lanceurs d'alerte est une mauvaise chose, d'une part, parce que sinon les divulgations se

---

200 Florian MARTIN-BARITEAU et Véronique NEWMAN, *Lancer une alerte au Canada : synthèse des connaissances*, 2018, en ligne : <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3112688>.

201 Voir, notamment, Loi facilitant la divulgation d'actes répréhensibles à l'égard des organismes publics (RLRQ, c. D-11.1); Loi concernant la lutte contre la corruption (RLRQ 2016, c. L-6.1); 1472 C.c.Q.

202 C'est notamment le cas dans la récente Loi belge où un signalement largement public (comme dans la presse) peut être autorisé : 1) que si gravité et urgence suffisante ou 2) si signalement privé préalable. Pour en savoir plus : <https://1819.brussels/infotheque/permis-reglementations-obligations/la-reglementation-sur-les-lanceurs-dalerte>.

203 Voir la Directive (UE) 2019/1937 du 23 octobre 2017 sur la protection des personnes qui signalent des violations du droit de l'Union.

204 Notamment pour les entreprises employant au moins cinquante salariés (art. 8 de la loi dites « Sapin 2 » (Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique)) ou à celles devant mettre en place un programme de conformité anticorruption (art. 8 de la loi dites « Sapin 2 »).

205 Sylvia LIU, « Data Privacy, Human Rights, and Algorithmic Opacity », (2022) 110 *California Law Review* 2087. D'ailleurs, la référence aux lanceurs d'alerte est expressément faite dans le DMA (considérants 42 et 102), et ce, même s'il n'y a aucun processus qui encadre son intervention (une directive de 2019 existe à cet égard et est citée au considérant 142).

206 Jean CATTAN et Joëlle TOLEDANO, « La Commission dans la mise en œuvre du DMA : citadelle assiégée ou chef d'orchestre ? », (2022) 3 *Concurrences* 3.

207 Dominique ROUSSEAU, « La figure multidimensionnelle du citoyen de la démocratie continue », dans Mathilde HEITZMANN-PATIN et Julien PADOVANI (dir.), *La participation du citoyen à la confection de la loi*, Mare & Martin, Paris, 2021, p. 165.

font publiquement et, d'autre part, parce que c'est le moyen de connaître des failles qui n'auraient pas été autrement connues[208].

Mises en application variées. En Europe, il semble néanmoins que la mise en place de tels cadres réglementaires soit assez lourde. Aussi, au-delà de la directive précitée, de lois[209], de décrets[210], des changements sont également intervenus au sein de certains corpus de règles. Par exemple, presque systématiquement, chaque dénonciation implique la divulgation de renseignements personnels ce qui amena certains organismes de protection des renseignements personnels, comme la CNIL en France, à mettre en place un référentiel pour organiser la divulgation de l'alerte[211]; référentiel qui est d'autant plus important qu'une analyse de risques est requise pour la mise en place d'un tel processus d'alerte[212]. Ce cadre est beaucoup plus lourd que ceux qui prévalent en Amérique, même par rapport au droit québécois qui est vu comme un acteur plutôt diligent à l'échelle du Canada[213], et ce, malgré la récente affaire *Robert*[214]. Aussi, « le diable est dans les détails » et c'est dans la mise en application des processus de lanceurs d'alerte que va dépendre l'efficacité de la mesure.

Lanceur d'alerte spécifique. Après, au regard du précédent critère de neutralité technologique, rien ne semble vraiment motiver la mise en place d'un processus spécifique qui puisse être attaché à la LCCJTI. En effet, d'une part, un processus général s'applique pour le secteur public[215]. D'autre part, l'expérience étrangère montre que pour les très grosses organisations privées, de type, GAFAM, il est difficile de croire qu'un processus de lanceur d'alerte non étatsuniens puisse être d'une certaine efficacité, et encore...[216]

---

208 Florian MARTIN-BARITEAU, « Acteurs de la justice: les lanceurs d'alerte », conférence du CRDP, 30 mars 2022, autour de la 34e minute, en ligne : <https://youtu.be/a6Dgscrq8DM?si=6FOYucOs9339lhV3>.

209 En France, on peut citer la Loi du 21 mars 2022 (Loi n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte).

210 Toujours en France, on peut citer le Décret d'application du 3 octobre 2022 (Décret n° 2022-1284 relatif aux procédures de recueil et de traitement des signalements émis par les lanceurs d'alerte et fixant la liste des autorités externes instituées par la *Loi n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte*).

211 Délibération nº 2023-064 du 6 juillet 2023 portant abrogation de la délibération nº 2019-139 du 18 juillet 2019 portant adoption d'un référentiel relatif aux traitements de données à caractère personnel destinés à la mise en œuvre d'un dispositif d'alertes professionnelles et adoption d'un référentiel relatif aux traitements de données à caractère personnel destinés à la mise en œuvre d'un dispositif d'alertes professionnelles. Pour en savoir plus, Blanche BALIAN et Laetitia GHEBALI, 15 septembre 2023, en ligne : <https://www.dalloz-actualite.fr/flash/cnil-mise-jour-du-referentiel-relatif-aux-dispositifs-d-alerte-professionnelle-suite-de-transp>.

212 Délibération n° 2018-327, 11 oct. 2018, D. 2019, 1673, observation Winston Maxwell et Célia Zolynski.

213 Florian MARTIN-BARITEAU, « Acteurs de la justice: les lanceurs d'alerte », conférence du CRDP, 30 mars 2022, en ligne : <https://youtu.be/a6Dgscrq8DM?si=6FOYucOs9339lhV3>.

214 PROTECTION DU CITOYEN, Application de la Loi facilitant la divulgation d'actes répréhensibles à l'égard des organismes publics : des manquements majeurs de la part du ministère de l'Agriculture, des Pêcheries et de l'Alimentation, 13 juin 2019, en ligne : <https://protecteurducitoyen.qc.ca/sites/default/files/pdf/rapports_speciaux/rapport-mapaq-manquements-traitement-divulgation.pdf>.

215 Loi facilitant la divulgation d'actes répréhensibles à l'égard des organismes publics (RLRQ, c. D-11.1).

216 Certaines affaires retentissantes, comme notamment le « coulage » de Frances Haugen relativement à Facebook, montrent que la publicisation est parfois la seule option véritable.

PROPOSITION #7 : La mise en place d'un processus spécifique de lanceur d'alerte ne semble pas de mise sous l'égide de la LCCJTI.

c) « Hackeurs » légaux

Début de tendance en cours. Vu comme une forme particulière de lanceurs d'alerte, le statut particulier des « bidouilleurs » (hackeurs) légaux, aussi dénommés « hackeurs éthiques » ou « hackeurs blancs » correspond à cette même volonté de faire participer des individus au processus de régulation, vu dans son ensemble. Le droit français fut l'un des premiers à légiférer, en 2016[217], sur la question suite à une jurisprudence montrant une indulgence modérée envers les accès non autorisés sans dommage[218]. En 2022, les États-Unis, sans modifier spécifiquement le CFAA, le Département de la Justice fédéral (DOJ) a révisé ses « *Prosecutorial Guidelines* » dès lors que des preuves existent sur le fait que l'intrusion avait manifestement une intention de bonne foi[219]. La Belgique a aussi effectué, tout récemment (15 février 2023), une avancée en instaurant un processus de dénonciation auprès d'un organisme étatique dédié[220] dont le régime semble être le plus abouti tant en termes de protection (confidentialité, immunité réelle), que des modalités de divulgation qui impliquent une certaine structuration administrative[221].

Spécificités québécoises. Au regard d'un intérêt manifesté au Québec[222], mais non officialisé au-delà du formulaire disponible pour le signalement de vulnérabilités techniques[223], il est intéressant de regarder les avancées opérées, notamment en Europe, pour là encore tenter de diversifier les capacités de contrôle des entités tant privées que publiques. Cela dit, une spécificité majeure est que le droit criminel étant de compétence fédérale, la mise en application d'une pareille mesure peut être difficile. Quant au regard de la question civile, il importe d'envisager si une telle intervention législative ne viendrait pas empiéter sur les règles de responsabilité civile

---

217 *Loi sur la république numérique* (2016), art. 47 qui se lit comme suit : « Pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'article 40 du code de procédure pénale n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule autorité nationale de sécurité des systèmes d'information une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données ».

218 Fabrice MATTATIA, « Faut-il dépénaliser les hackers blancs ? », (2015) 4 *Revue de science criminelle et de droit comparé* 837, en ligne : <https://www.cairn.info/revue-de-science-criminelle-et-de-droit-penal-compare-2015-4-page-837.htm>.

219 *Computer Fraud and Abuse Act* précise que « The attorney for the government should decline prosecution if available evidence shows the defendant's conduct consisted of, and the defendant intended, good-faith security research », en ligne : <https://www.justice.gov/opa/press-release/file/1507126/download>

220 Pour en savoir plus, voir le site du CCB (Center for Cybersecurity of Belgium) qui reçoit les dénonciations de vulnérabilités, en ligne : <https://ccb.belgium.be/fr/actualit%C3%A9/nouveau-cadre-juridique-pour-le-signalement-de-vuln%C3%A9rabilit%C3%A9-informatique>.

221 Plateforme dédiée (comme d'ailleurs au regard du droit français), formulaire ad hoc, non destruction et non divulgation des données, etc.

222 Conférence de presse de M. Éric Caire, ministre responsable de l'Accès à l'information et de la Protection des renseignements personnels, 1er octobre 2021, en ligne : <https://www.assnat.qc.ca/fr/actualites-salle-presse/conferences-points-presse/ConferencePointPresse-77091.html>.

223 Voir le formulaire disponible auprès du Centre gouvernemental de cyberdéfense : signalement des vulnérabilités, en ligne : <https://www.cyber.gouv.qc.ca/signalements/signalement-vulnerabilites>.

traditionnelles et, notamment, l'article 1457 C.c.Q. En effet, une intrusion de bonne foi et sans dommages pourrait de surcroît ne pas être constitutive de faute. Après, au-delà du droit, il importe de se demander si une telle intervention législative ne pourrait pas avoir un effet « éducatif » auprès de la communauté en permettant à la fois de sensibiliser l'importance de la sécurité et de dévoiler certaines failles.

PROPOSITION #8 : Au regard de spécificités québécoises, une étude de la pertinence du « hacking légal » doit être envisagée tant au niveau légal, éducatif et administratif.

2.1.1.2.2 Tendances plus innovantes

Des avenues à explorer. Même si le terme « innovation » est quelque peu galvaudé, de par son indéfinition, son caractère à la mode, voire le libéralisme qui le caractérise souvent[224], il est souvent instrumentalisé pour réguler les phénomènes technologiques; une tendance forte est donc de réguler le neuf par le neuf. Parmi les avenues observées, nous croyons nécessaire de traiter deux phénomènes, deux termes, qui représentent ces appétits d'innovation, à savoir les bacs à sable réglementaires et les « RegTechs ».

2.1.1.2.2.1 Hypothèse des « bacs à sable réglementaires » (Sandboxes)

Définition du bac à sable réglementaire. Alors qu'elle semble très en lien avec l'approche participative préalablement décrite, une solution qui a été assez généralement suivie, tant en Amérique du Nord qu'en Europe, est celle des bacs à sable réglementaires. Souvent vus comme un « nouvel arsenal réglementaire »[225], par cette expression, on entend un projet expérimental où on teste un cadre réglementaire généralement à un domaine d'application particulier. Pour une période déterminée, on invite à une réflexion un certain nombre d'acteurs afin de participer à l'élaboration de règles. On peut donc le définir :

> « as a legislative or regulatory instrument of a temporary nature with limited geographic and/or subject application which is designed to test a new policy or legal solution and includes the prospect of an evaluation at the end of the experimental period. »[226]

Un bac à sable réglementaire est aussi généralement associé à une institution, presque toujours nationale, même si des perspectives plus internationales semblent conseillées ultérieurement[227].

---

224 Thierry MÉNISSIER, *Innovations. Une enquête philosophique*, Paris, Hermann, 2021.

225 Chris BRUMMER et Yesha YADAV, « Fintech and the Innovation Trilemma », (2017) 107 *GEO. L.J.* 235, à la page 291.

226 Sofia RANCHORDÁS, « Experimental Regulations for AI : Sandboxes for Morals and Mores », dans *Morals and Machines*, 2021, p. 86, en ligne : <https://iris.luiss.it/bitstream/11385/210516/1/2747-5174-2021-1-86.pdf>, aux pages 91-92.

227 OECD, *Regulatory Sandboxes in Artificial Intelligence*, juillet 2023, *OECD Digital Economy Papers*, n° 356, en ligne : <https://www.oecd.org/publications/regulatory-sandboxes-in-artificial-intelligence-8f80a0e6-en.htm>, p. 28. Ce rapport évoque un exemple espagnol où une phase nationale est lancée en matière de régulation des SIA (systèmes d'intelligence artificielle), tout en prévoyant à terme une seconde phase internationale.

Raisons d'être. La démarche est à la mode[228]. Le mot aussi. Et le monde des technologies a toujours été friand de ces néologismes parfois vides de sens. Après, le phénomène n'est pas pleinement nouveau, celui-ci correspondant aux projets de lois expérimentales qui furent parfois mises en place aussi loin que dans les années 1980[229]. En fait, le procédé est souvent envisagé comme un moyen de se prémunir contre les carences des moyens traditionnels et, à premier titre, des formes traditionnelles de réglementation (lois et règlements). Ces dernières, du fait parfois de la longueur et lourdeur des processus[230], d'a priori critiques, sont jugées à tort mal adaptées pour les domaines techniques. Aussi, il est étonnant de constater que la doctrine et surtout les documents à saveur exploratoire (« white papers », études, rapports, etc.) semblent particulièrement en faveur d'un tel procédé. Sans remettre en cause cette appétence pour ce mode de fonctionnement, au contraire, tout comme l'approche participative, il importe d'apporter un regard critique et analytique sur une manière de faire qui ne dispose pas de surcroît d'un recul pour véritablement tester sa pertinence. D'autant que les preuves de leur effectivité demeurent encore minces[231]. Plus précisément, les avantages basés sur l'expérience des fintechs sont plus en lien avec la hausse de la concurrence (notamment la facilité à faire rentrer de nouveaux produits sur le marché) que sur la régulation à proprement parler[232].

Terrains propices. Issus dans un premier temps du monde des « fintechs »[233], qui constitue toujours un terrain propice[234], les bacs à sable réglementaires sont souvent justifiés d'environnements qui présentent des hauts niveaux d'incertitude. On le trouve également beaucoup dans le cas des professions juridiques, notamment lorsque celles-ci sont confrontées aux technologies[235]. On peut notamment citer le cas du Barreau du Québec qui a souhaité en élaborer un concernant l'usage de l'intelligence artificielle[236], domaine également particulièrement propice à cette solution. En effet, l'évolution rapide du domaine, sa nouveauté, sa complexité, autant de caractéristiques

---

228 Cristie FORD and Quinn ASHKENAZY, « The Legal Innovation Sandbox », *Allard Research Commons*, 2023, p. 1, en ligne : <https://commons.allard.ubc.ca/fac_pubs/712/>.

229 Sofia RANCHORDÁS, « Experimental Regulations for AI : Sandboxes for Morals and Mores », dans *Morals and Machines*, 2021, p. 86, en ligne : <https://iris.luiss.it/bitstream/11385/210516/1/2747-5174-2021-1-86.pdf>, à la p. 91.

230 On peut penser à la difficulté de voir des lois être adoptées aux États-Unis ou au Canada où, au-delà d'un réflexe législatif moindre, en matière technologique. *Supra*, Section 2.1.1.1.2.

231 Cristie FORD and Quinn ASHKENAZY, « The Legal Innovation Sandbox », *Allard Research Commons*, 2023, p. 9, en ligne : <https://commons.allard.ubc.ca/fac_pubs/712/>.

232 Cristie FORD and Quinn ASHKENAZY, « The Legal Innovation Sandbox », *Allard Research Commons*, 2023, p. 1, en ligne : <https://commons.allard.ubc.ca/fac_pubs/712/>, page 12. FINANCIAL CONDUCT AUTHORITY (FCA), *The Impact and Effectiveness of Innovate*, (2019), en ligne : <www.fca.org.uk/publication/research/the-impact-and-effectiveness-of-innovate.pdf>, (voir notamment le point 2.1).

233 FINANCIAL CONDUCT AUTHORITY (FCA), « Regulatory Sandbox », (2015), en ligne : <https://www.fca.org.uk/publication/research/regulatory-sandbox.pdf>.

234 Cristie FORD and Quinn ASHKENAZY, « The Legal Innovation Sandbox », *Allard Research Commons*, 2023, p. 1, en ligne : <https://commons.allard.ubc.ca/fac_pubs/712/>, p. 9. On peut y lire qu'en novembre 2020, 73 bacs réglementaires existent à travers le monde dans ce domaine dans 57 juridictions différentes.

235 Cristie FORD and Quinn ASHKENAZY, « The Legal Innovation Sandbox », *Allard Research Commons*, 2023, p. 1, en ligne : <https://commons.allard.ubc.ca/fac_pubs/712/>, p. 16 et ss.

236 *Id.*, p. 18.

vues précédemment[237], font que les questionnements du cadre légal applicable s'appliquent à une « cible mouvante »[238] et difficile à appréhender. Les cadres réglementaires ayant trait à la protection des renseignements personnels ont aussi donné lieu à de multiples expériences tout comme les voitures autonomes[239].

« **Au-delà du droit** ». En plus de certains secteurs d'activité en particulier, les bacs à sable réglementaires sont davantage sur le droit informel que sur le droit « dur » :

> « Sandboxes should not be used only to validate hard-law expectations, but also to support open innovation. Regulatory sandboxes should be implemented as complementary tools alongside existing innovation institutions, notably innovation hubs. »[240]

Fonctions du bac à sable réglementaire. En conformité avec l'approche fonctionnelle précitée[241], il importe de s'arrêter à ce qu'autorise un tel procédé. De façon assez commune, il est intéressant de constater que son objectif suprême est de constituer un espace de réflexion permettant d'effectuer un équilibre entre innovation et protection. Deux fonctions contraires qui sont fondamentales, même implicitement dans le présent mandat qui nous est donné de mener, mais dont les critères pour les départager sont loin d'être aisés à identifier. En fait, les bacs à sable réglementaires sont souvent davantage associés à un rôle d'accompagnement que de sanction[242]; situation qui est loin d'être neutre. Le bac à sable a donc une vertu substantielle : il constitue le moyen de voir révéler des règles pour lesquelles des doutes subsistent; pour lesquelles des tests doivent être validés. Mais ce n'est pas tout. Ils sont également préconisés afin de densifier des règles applicables et, notamment, lorsqu'il s'agit de les rendre accessibles à des acteurs qui ne sont pas toujours à même de les créer eux-mêmes. À titre d'exemple, les plus petites structures commerciales dans le domaine de l'intelligence artificielle sont souvent perdues quant aux cadres réglementaires qui s'appliquent à leur situation[243]. Les bacs à sable réglementaires sont donc aussi un moyen d'améliorer la concurrence[244].

---

237 *Supra*, Section 1.2.2.1.

238 Sofia RANCHORDÁS, « Experimental Regulations for AI: Sandboxes for Morals and Mores », *Morals and Machines*, 2021, p. 86, à la page 88, en ligne :<https://iris.luiss.it/bitstream/11385/210516/1/2747-5174-2021-1-86.pdf>.

239 BMWi, 2019.

240 OECD, « Regulatory Sandboxes in Artificial Intelligence », juillet 2023, *OECD Digital Economy Papers*, n° 356, en ligne : <https://www.oecd.org/publications/regulatory-sandboxes-in-artificial-intelligence-8f80a0e6-en.htm>, p. 25.

241 *Supra*, Section 1.2.3.1.

242 Deirdre AHERN, *Regulators Nurturing Fintech Innovation: Global Evolution of the Regulatory Sandbox as Opportunity-Based Regulation*, European Banking Institute, Working Paper Series nº 60, 2020, p. 11 : « Provision of a regulatory sandbox sees a regulator moving from the role of gatekeeper to quasi-compliance consultant and ally ».

243 On peut par exemple penser à la situation que l'on aperçoit dans le jugement de la CAI concernant la Commission scolaire Val de Cerf où la relative petite taille du projet impliquait un cadre réglementaire qui réclamait des ressources supérieures au coût de développement.

244 OECD, « Regulatory Sandboxes in Artificial Intelligence », juillet 2023, *OECD Digital Economy Papers*, n° 356, en ligne : <https://www.oecd.org/publications/regulatory-sandboxes-in-artificial-intelligence-8f80a0e6-en.htm>.

Intégration dans les textes de lois. Au-delà de l'appréhension assez vague de cette notion, il est étonnant de constater qu'en dépit des différences de vue entre l'Europe et l'Amérique, la solution est envisagée sur les deux continents. Si l'origine est plutôt américaine, on la trouve néanmoins expressément formulée dans le récent *Règlement européen sur l'intelligence artificielle* où trois articles spécifiques encadrent le procédé :

> « **53.** Les autorités d'établissement fournissent aux fournisseurs potentiels de bacs à sable réglementaires qui développent des systèmes d'IA à haut risque des orientations et une supervision concernant la manière de satisfaire aux exigences prévues dans le présent règlement, de sorte que les systèmes d'IA puissent quitter le bac à sable étant dans une situation de présomption de conformité aux exigences spécifiques du présent règlement qui ont été évaluées dans le bac à sable. [...]. »

Cela dit, l'article 53 introduit une simple opportunité; guère plus et sans vraiment déterminer ce à quoi il sert[245].

Garanties. Même si l'exercice sort du cadre de cette étude, il va sans dire que l'élaboration d'un bac à sable réglementaire implique la mise en place d'un certain nombre de garanties afin de compenser l'informalité du processus. Des garanties qui impliquent une structuration nécessaire[246] qui vient combler l'inhérente fragilité que tout processus communautaire implique. Or, au regard des tendances constatées, notamment dans les textes de lois, peu de directions transparaissent, la plupart renvoyant à des textes subséquents le soin de définir le *modus operandi*[247]. Tout se joue donc dans la manière de mettre en œuvre[248]. Parmi les garanties qui peuvent être mises en place, nous retiendrons les suivantes :

- **Institutionnalisation.** Les bacs à sable, c'est souvent une critique, sont trop souvent vus comme un moyen pour l'État de se désengager. Au contraire, une institutionnalisation semble de mise afin d'assurer son succès.
- **Modalités de sélection**. Il est possible de prévoir des critères précis pour déterminer les personnes conviées, et ce, pour des fins de représentation, de légitimité, d'inclusion, etc. Malheureusement, cette démarche semble peu satisfaite à elle seule[249].

---

245 Wolf-Georg RINGE, *Why We Need a Regulatory Sandbox for AI*, Oxford Law Blogs, 2023.

246 Cristie FORD and Quinn ASHKENAZY, « The Legal Innovation Sandbox », *Allard Research Commons*, 2023, p. 5, en ligne : <https://commons.allard.ubc.ca/fac_pubs/712/>.

247 Voir notamment le *Règlement européen sur l'intelligence artificielle*, art. 53 et ss.

248 Cristie FORD and Quinn ASHKENAZY, « The Legal Innovation Sandbox », *Allard Research Commons*, 2023, p. 6, en ligne : <https://commons.allard.ubc.ca/fac_pubs/712/>: « As is so often the case with regulation, the difference between a permissive free-for-all that undermines regulatory priorities, and a careful experiment that stands to enhance legal service provision while also enhancing regulatory understanding, comes down to implementation ».

249 OECD, « Regulatory Sandboxes in Artificial Intelligence », juillet 2023, *OECD Digital Economy Papers*, n° 356, en ligne : <https://www.oecd.org/publications/regulatory-sandboxes-in-artificial-intelligence-8f80a0e6-en.htm>, p. 23. Ce rapport prend l'exemple où un bac à sable réglementaire de l'ICO Britannique en 2019 avait permis de constater que seulement 10 des membres (sur 69) avaient été invités sur la base de critères précis.

- **Consensus et dissensus**. Si les standards nationaux et internationaux visent à élaborer des consensus, dans le cadre de tels espaces, il importe de ne pas se limiter à l'élaboration de tels accords. Il nous semble aussi important de bien connaître les points qui achoppent.
- **Transparence du processus**. Tout le cycle de vie du bac à sable (de sa création à sa dissolution) doit donner lieu à un haut niveau de transparence. Si cela se comprend bien au début notamment avec les modalités de sélection précitées, il est également important de tirer profit de l'ensemble du processus en collectant des données sur ses avantages et inconvénients[250].
- **Ressources**. Pour la durée du projet de bac à sable réglementaire, il importe de donner les moyens de ses ambitions au bac à sable. Parmi les moyens possibles, on peut penser à la capacité d'effectuer des recherches, des sondages, etc.[251] De façon plus institutionnelle, il peut aussi être pertinent d'avoir un administrateur en charge du bac à sable qui dispose de vrais pouvoirs d'organisation[252]. En d'autres mots, la motivation première des bacs à sable réglementaires n'est pas de permettre aux institutions publiques de s'exonérer de toutes démarches de régulation.
- Etc.

PROPOSITION #9 : La pertinence des « bacs à sable réglementaires » doit être considérée dans des domaines où le besoin de réglementation est particulièrement utile. L'intelligence artificielle constitue un exemple où un tel besoin peut se faire sentir.

2.1.1.2.2.2 Hypothèse des « RegTechs »

Définition. De façon plus succincte, nous croyons aussi important de développer rapidement quelques propos sur ce qui se dénomme généralement les « RegTechs ». Derrière ce néologisme, on entend des solutions plus ou moins automatisées qui permettent de vérifier le respect des règles par une institution. Certes, ce phénomène origine du monde de la finance et du droit bancaire, mais il est intéressant car il s'agit de domaines :

- substantiellement encadrés par le droit, du fait d'enjeux d'envergure;
- où les obligations d'auto-déclaration par les parties elles-mêmes sont très courantes sous l'appellation de « compliance » (conformité), et ce, bien avant que cela se généralise dans l'ensemble des questions touchant au numérique (responsabilité, preuve, sécurité, identité);
- fortement numérisés (30 % des dépenses des banques sont en lien avec le numérique);
- qui disposent d'un certain recul car cela fait déjà de nombreuses années que ce phénomène se constate.

---

250 Cristie FORD and Quinn ASHKENAZY, « The Legal Innovation Sandbox », *Allard Research Commons*, 2023, p. 1, en ligne : <https://commons.allard.ubc.ca/fac_pubs/712/>, p. 53.

251 *Id.*, p. 52.

252 *Id.*, p. 55.

Aussi, au regard de la hausse constante de cette obligation d'auto-proclamation[253], l'idée est rapidement venue qu'il serait judicieux de faire intervenir des outils technologiques capables d'aider à dévoiler la diligence des acteurs. Le numérique généralisant l'idée selon laquelle il importe de faire « une preuve à soi-même » ou « par soi-même », ce travail de documentation assez laborieux trouve avec les technologies : « a host of arrangements that seek to facilitate the management of reporting and compliance »[254].

Concrètement, les « RegTechs » correspondent à des applications détenant des degrés variés d'intelligences automatisées permettant d'évaluer des risques, notamment en matière de blanchiment d'argent, d'offrir des interprétations automatiques analysant des courriels, voire des messages vocaux, de mesurer la capacité des outils mis en place à déceler les bris de sécurité, le tout permettant de faciliter la mise en preuve des documentations requises. Nous croyons important de mentionner dans le présent rapport cette tendance mondiale des « RegTechs » dans la mesure où ce choix technologique n'est pas neutre et constitue, de par cette généralisation de l'auto-déclaration des entités contrôlées « a pivotal change leading to a paradigm shift in regulation »[255].

Visions critiques. Si l'idée est intéressante, l'utilisation des « RegTechs » donne lieu à des visions quelque peu critiques. **En premier lieu**, il faut noter que peu de lois sont intervenues sur le sujet et si l'Europe est un fer de lance en matière de régulation des technologies, la numérisation des finances donne lieu surtout à des documents internes et études des organismes de contrôle[256]. **En deuxième lieu**, les documentations produites pour fin de conformité sont parfois très difficiles à comprendre, et ce, en concordance avec les enjeux d'explicabilité qui ne manquent pas de poindre dès lors que l'on touche aux questions d'intelligence artificielle.

> « The American experience of the 2008 financial crisis offers an instructive illustration of how the lack of human supervision over bank's automated risk-assessment processes facilitated regulatory violations. »[257]

Une opacité qui est accrue par le fait que de plus en plus souvent le travail de documentation (reporting) est effectué par une sous-traitance spécialisée à laquelle les banques s'adonnent souvent afin d'effectuer ce travail de conformité[258]. **En troisième lieu**, les manières de faire sont parfois si dispersées que l'on constate à la fois un besoin d'uniformisation que d'un meilleur partage du savoir-faire. L'EBA (European Banking Authority) identifie clairement dans un rapport de 2021

---

253 Anastasia KONINA,« Banks as Delegated Regulators of Technology », (2022) 59-3 *Alberta Law Review* 753, 754.

254 *Id.*

255 Douglas ARNER, Janos BARBERIS and Ross BUCKLEY, « FinTech, RegTech, and the Reconceptualization of Financial Regulation », (2017) 37-3 *Northwestern Journal of International Law and Business* 371, à la page 382.

256 Jonathan MCCARTHY, « The Regulation of RegTech and SupTech in Finance: ensuring Consistency in Principle and Practice », (2023) 31-2 *Journal of Financial Regulation and Compliance* 186-199, 187.

257 Anastasia KONINA, « Banks as Delegated Regulators of Technology », (2022) 59-3 *Alberta Law Review* 753, 756. L'autrice cite notamment Tom CW Lin, « The New Financial Industry », (2014) 65-3 *Alabama Law Review* 567, 579-580.

258 OFFICE OF THE SUPERINTENDENT OF FINANCIAL INSTITUTIONS (OSFI), *Developing Financial Sector Resilience in a Digital World: Selected Themes in Technology and Related Risks*, Ottawa, 2020.

des besoins en ce sens[259] qui, selon elle, peut même aller jusqu'à la certification : « for convergence of regulatory standards, backed by the knowledge-gathering activities of the European Forum for Innovation Facilitators (EFIF) »[260].

Notons qu'un besoin d'uniformisation est également revendiqué par la Banque d'Angleterre[261]. **En quatrième lieu**, la complexité inhérente à de tels processus fait en sorte que la solution, originellement choisie pour des raisons d'efficacité, atteint des niveaux de sophistication si élevés qu'il est impossible de l'étendre à de plus petites structures. Surtout que les tiers qui offrent des services de « reporting » disposent souvent d'un ancrage international très marqué[262].

Apprentissages. Nous voulions parler des « RegTechs » car elles montrent que très souvent le « centre de gravité normatif » se situe auprès des acteurs eux-mêmes qui, s'ils disposent du fait des lois de l'obligation de produire des documentations internes, ont parfois de la difficulté, d'une part, à identifier les normes informelles (standards) sur lesquelles se baser et, d'autre part, de modèle qui pourrait faciliter ce travail de documentation, notamment pour les plus petites structures. Aussi, la place des organismes de contrôle est revendiquée[263], ceux-ci devant se commettre dans l'élaboration de ces « guides » nécessaires à l'industrie.

L'avènement de la notion de « SupTech ». Si les « RegTechs » présentent des enjeux transposables au domaine du numérique dans leur ensemble, il importe aussi d'évoquer une notion distincte mais non sans lien, à savoir les « SupTechs ». Par ce néologisme, constituant une contraction de « supervision » et technologies, on entend l'usage « of innovative technologies to support supervision » et ainsi permettre aux autorités de contrôle « to digitise reporting and regulatory process »[264]. Cette notion renforce le besoin de l'industrie de disposer de moyens pour l'aider à se conformer aux règles applicables.

Illustrations. Aussi, et afin d'aider l'industrie à mieux « se » réguler, il importe de regarder des exemples où les organismes de contrôle propose, notamment, des standards et modèles capables de diriger et d'accompagner les acteurs. Sans prétention d'exhaustivité, on peut citer l'« AI Verify

---

259 EBA, « Analysis of RegTech in the EU Financial Sector », 2021, p. 78.

260 Jonathan Mccarthy, « The Regulation of RegTech and SupTech in Finance: ensuring Consistency in Principle and Practice », (2023) 31-2 *Journal of Financial Regulation and Compliance* 186-199, 188.

261 BANK OF ENGLAND, « Bank of England Plan: Transforming Data Collection from the UK Financial Sector », 2021.

262 Jonathan MCCARTHY, « The Regulation of RegTech and SupTech in Finance: ensuring Consistency in Principle and Practice », (2023) 31-2 *Journal of Financial Regulation and Compliance* 186-199, 191.

263 Jonathan MCCARTHY, « The Regulation of RegTech and SupTech in Finance : ensuring Consistency in Principle and Practice », (2023) 31-2 *Journal of Financial Regulation and Compliance* 186-199, évoque les limites d'une approche où les acteurs disposent d'une trop grande liberté pour agir et demande le maintien d'une approche « top-down » capable de « guider » les acteurs. Voir aussi Anastasia KONINA, « Banks as Delegated Regulators of Technology », (2022) 59-3 *Alberta Law Review* 753.

264 EUROPEAN COMMISSION, « A European Finance Strategy for EU », COM 2020, 591, p. 13.

ToolKit » qui constitue un logiciel *open source* qui sert à évaluer la fiabilité de SIA[265] ou le modèle d'EFVP automatisée proposé par la CNIL[266].

Apprentissage. Ces exemples confortent l'idée que l'industrie, notamment les plus petites et moyennes organisations, est en quête de cadres tant au niveau informel qu'applicatif pour l'aider à se conformer aux règles applicables.

> « "bottom-up" standardisation still requires clear "top-down" intervention to give guidance on how organisations should adjust their governance and oversight procedures around RegTech and SupTech tools. »[267]

Cet appel à une intervention étatique sur tous les niveaux de normativité (formel – informel – individuel), et pas uniquement pour les normes législatives et réglementaires (c'est-à-dire formelles), est à lier à nos précédents propos sur le Comité d'harmonisation et à son rôle d'animation normative[268].

2.1.1.2.2.3 Hypothèse de remise en cause des « silos »

Silos. Enfin, pour finir, et même si cela peut tenir de l'évidence tant cette prétention est réclamée depuis longtemps, il importe de ne pas reproduire la pratique des « silos » qui font en sorte que trop souvent, au sein d'une même institution, la communication des manières de faire et des politiques internes ne se s'opère pas[269]. Alors que ce type de coopération est désormais revendiqué[270], elle se conçoit en l'occurrence relativement aux documentations internes qui se doivent d'être systématiquement rédigées et dont, trop souvent, les institutions confectionnent dès le début, n'ayant pas de modèle sur lequel se baser au départ.

2.2 LCCJTI + responsabilité

Renforcer les libertés expressives. Lorsque les lois répartissant la responsabilité pour les activités se déroulant sur Internet ont été mises en place dans les années 1990, les législateurs européens et américains souhaitaient un cadre légal qui renforcerait la liberté de chaque individu de s'exprimer. Pour cette raison, on a évité d'imposer aux intermédiaires (à l'époque, il s'agissait surtout des sites qui hébergeaient des blogues) une responsabilité trop lourde pour les propos ou les images émanant

---

265 OECD, « Regulatory Sandboxes in Artificial Intelligence », juillet 2023, *OECD Digital Economy Papers*, n° 356, en ligne : <https://www.oecd.org/publications/regulatory-sandboxes-in-artificial-intelligence-8f80a0e6-en.htm>, p. 26.

266 Pour en savoir plus, voir en ligne : <https://cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil>.

267 Jonathan MCCARTHY, « The Regulation of RegTech and SupTech in Finance : Ensuring Consistency in Principle and Practice », (2023) 31-2 *Journal of Financial Regulation and Compliance* 186-199, 192.

268 *Supra*, Section 2.1.1.1.1.

269 Pierre TRUDEL, « Améliorer la protection de la vie privée dans l'administration électronique : pistes afin d'ajuster le droit aux réalités de l'État en réseau, réalisé pour le ministère des Relations avec les citoyens et de l'immigration », mars 2003.

270 SECRÉTARIAT DU CONSEIL DU TRÉSOR, *Stratégies de transformation numérique gouvernementale, 2019-2023*, Québec, 2019, en ligne : <https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/secretariat-du-conseil-du-tresor/publications-adm/strategie/StrategieTNG.pdf>, p. 10.

de tiers. Aux États-Unis, dans les années 1990, le Congrès a adopté une loi qui exonère presque totalement les plateformes de toute responsabilité pour propos et comportements délictueux émanant de tiers qui utilisent leurs sites pour mettre des contenus en ligne. En Europe et au Québec, on a opté pour des règles prescrivant que les intermédiaires ne sont responsables qu'à compter du moment où ils ont connaissance du caractère illicite des propos ou des activités menées sur leur plateforme.

Responsabilité conditionnelle. La LCCJTI formule les règles à l'égard de tout prestataire de services qui se trouve effectivement dans la situation décrite, qui pose ou ne pose pas les gestes mentionnés dans la Loi. Ces prestataires sont :

- le prestataire offrant des services de conservation de documents technologiques sur un réseau de communication. L'archétype de ce prestataire est l'hébergeur, mais la notion est assez large pour viser l'ensemble des prestataires qui accueillent des documents qu'ils conservent et qui sont mis à disposition sur le réseau. Par exemple, les environnements à contenu généré par les utilisateurs correspondent à cette description (art. 22);
- le prestataire offrant des services de référence à des documents technologiques, dont un index, des hyperliens, des répertoires ou des outils de recherche (art. 22);
- le prestataire fournissant les services d'un réseau de communication exclusivement pour la transmission de documents technologiques. Nous désignerons cet intermédiaire par le mot transmetteur (art. 36);
- l'intermédiaire qui conserve les documents à la seule fin d'assurer l'efficacité de la transmission. On vise, dans cette catégorie, le prestataire qui agit à titre d'intermédiaire pour conserver sur un réseau de communication les documents technologiques que lui fournit son client, et qui ne les conserve qu'à la seule fin d'assurer l'efficacité de leur transmission ultérieure aux personnes qui ont droit d'accès à l'information (art. 37)[271].

Application. Le régime de limitation de la responsabilité de ces intermédiaires s'applique aux matières relevant de la compétence du Parlement du Québec. La Loi vient expressément exclure certaines obligations à la charge des intermédiaires, afin de délimiter le champ de ce qui peut constituer un comportement susceptible d'engager leur responsabilité.

Régime spécifique. Les articles 22, 26, 27, 36 et 37 de la LCCJTI instaurent un régime spécifique de responsabilité en faveur de certains intermédiaires techniques. Les prestataires de services impliqués dans la communication de documents bénéficient, moyennant le respect de certaines conditions, d'un régime de responsabilité fondé sur la connaissance du caractère illicite des documents transmis. Ce régime de responsabilité s'applique lorsque certaines conditions sont établies[272]. Ces conditions sont relatives au contrôle et à la connaissance des documents, de leur caractère fautif ou illicite. L'exercice du contrôle à l'égard de la diffusion d'une information s'assimile à l'exercice de la fonction éditoriale. L'exercice d'une telle fonction emporte forcément

---

271 Nicolas W. VERMEYS, *Droit codifié et nouvelles technologies : le Code civil*, Montréal, Éditions Yvon Blais, 2015, pp. 130-131.

272 Pierre TRUDEL, *Introduction à la loi concernant le cadre juridique des technologies de l'information*, Cowansville, Éditions Yvon Blais, 2012, pp. 216 et ss.

la connaissance de la teneur et de la nature du document. Le contrôle à l'égard d'un document implique le pouvoir de choisir ce qui sera diffusé, de décider de le diffuser et de décider à qui ou auprès de qui l'information sera diffusée[273]. De ce pouvoir de contrôle découle la responsabilité pour la transmission d'informations dommageables.

Pas d'obligation de surveiller. Comme le relevait la décision *A.B.* c. *Google*[274], la responsabilité de l'intermédiaire au regard de la LCCJTI n'est pas fondée sur une faute qu'il aurait pu commettre en tant que « fournisseur de contenu informationnel », mais plutôt sur le non-respect de ses obligations en tant qu'« intermédiaire fournissant des services de référence à des documents technologiques ». Ainsi, si un intermédiaire ne peut être tenu responsable du comportement du fournisseur de contenu et n'a aucune obligation positive de surveiller l'ensemble du contenu auquel son moteur de recherche fait référence, il a une responsabilité potentielle une fois qu'il a pris connaissance que les services qu'il procure sont utilisés pour une activité illicite.

2.2.1 États des tendances

Évolutions. Depuis 2001, le contexte de la responsabilité des intermédiaires a connu d'importantes évolutions. Les prestataires décrits à l'article 22 de la LCCJTI concernent aussi bien ceux qui conservent des documents pour autrui que des plateformes qui accueillent textes, sons, vidéos ou propositions d'entrer en relation contractuelle.

Acteurs majeurs. On a souligné que les plateformes numériques actuelles diffèrent grandement des intermédiaires techniques visés par les textes législatifs adoptés à la fin du siècle dernier[275]. En effet, ces intermédiaires sont devenus des multinationales dotées d'une puissance considérable. Ces entreprises disposent également d'un contrôle important sur les données et, enfin, la technologie permet une surveillance qui n'était pas envisageable il y a deux décennies. En raison de ces évolutions, la déresponsabilisation des intermédiaires techniques en général et des plateformes numériques en particulier est fréquemment remise en question. On observe d'ailleurs une tendance à préconiser un accroissement des obligations de ces acteurs dans différents secteurs.

2.2.1.1 La valorisation des données massives

Valorisation. Alors que la vision qui prévalait au début du siècle envisageait les intermédiaires comme des personnes qui mettaient en ligne un espace dans lequel les tiers pouvaient s'exprimer, les plateformes sont devenues au cours des deux dernières décennies des entreprises qui fonctionnent selon un modèle d'affaires consistant à valoriser les données massives générées par les mouvements de personnes qui évoluent sur leurs environnements. Les procédés, fondés sur les algorithmes et l'intelligence artificielle par lesquels les informations sont « poussées » ou proposées aux usagers, ont permis l'émergence de plateformes fonctionnant selon des modèles d'affaires reposant sur la valorisation des données produites par les usagers. L'enjeu ne concerne

---

273 Vincent GAUTRAIS et Pierre TRUDEL, *Circulation des renseignements personnels et Web 2.0*, Montréal, Éditions Thémis, 2010.

274 *A.B.* c. *Google*, 2023 QCCS 1167.

275 Vincent GAUTRAIS, Nicolas VERMEYS, Édouard HABIB et Kenza SASSI, *Revue de littérature en matière de régulation des plateformes numériques*, Rapport final combiné à l'attention du ministère de la Justice du Canada, 11 juillet 2019, p.18.

pas uniquement les données personnelles, mais aussi l'ensemble des données générées par le fonctionnement des environnements connectés[276]. Dans son ouvrage *L'âge du capitalisme de surveillance*[277], l'économiste Shoshana Zuboff explique que :

> « L'industrie numérique prospère grâce à un principe presque enfantin : extraire les données personnelles et vendre aux annonceurs des prédictions sur le comportement des utilisateurs. Mais, pour que les profits croissent, le pronostic doit se changer en certitude. Pour cela, il ne suffit plus de prévoir : il s'agit désormais de modifier à grande échelle les conduites humaines. »

Selon Shoshana Zuboff, ces capacités accrues de capter et d'analyser les données et les possibilités de prédiction qui en découlent mettent à mal aussi bien les libertés individuelles que le fonctionnement de la démocratie. Le fait que les plateformes tirent bénéfice des données produites ou traitées dans leurs espaces porte à s'interroger sur les types de devoirs et autres contreparties qui devraient leur incomber. Car les activités sur les plateformes permettent à celles-ci de valoriser les données, mais elles engendrent aussi des externalités négatives. D'où l'intérêt d'envisager leurs responsabilités en considérant les risques associés aux activités dont elles sont le théâtre.

2.2.1.2 Les plateformes mettent le public à risque

Enjeux collectifs. Les enjeux de responsabilité des intermédiaires ne se posent pas seulement au plan individuel. Un vaste ensemble d'activités se déroulant sur les plateformes en ligne présentent des risques pour le public. La facilité avec laquelle des contenus préjudiciables peuvent être partagés et amplifiés sur les plateformes d'Internet constitue un défi de taille. Dans une société de plus en plus connectée, les lois doivent établir un juste équilibre entre le maintien d'un espace libre et ouvert pour l'échange d'idées et d'information et le respect et la protection des droits et libertés individuels et collectifs. C'est là que se pose l'importante question des droits et des responsabilités des plateformes intermédiaires. Quelles sont leurs responsabilités à l'égard de l'exactitude et de la loyauté de l'information qui est distribuée ou partagée sur leurs plateformes, de même que de tous les méfaits sociaux pouvant en découler ? L'importance que prennent désormais des entreprises comme *Facebook* et *Google* a bouleversé cette distinction classique entre les « hébergeurs » de contenus, aux responsabilités limitées, et les « éditeurs » de contenus, responsables de tout ce qu'ils publient. Une tendance émerge de reconnaître aux intermédiaires certaines obligations de mesurer les risques auxquels sont exposés leurs utilisateurs et de faire les meilleurs efforts pour les gérer.

2.2.1.3 Les manipulations, fraudes et hypertrucages

Risque. La fabrication des hypertrucages est désormais à la portée de beaucoup de monde. Chaque jour, des faussetés délirantes sont diffusées et se répandent à la manière des virus sur les réseaux sociaux. L'existence des formidables possibilités de générateurs de faux portraits et de portraits stylisés (comme l'application *Lensa AI*) a contribué à faciliter la tâche de ceux qui diffusent des fausses informations sur Internet. Le risque de manipulation est l'un de ceux qui semble le plus

---

276 Voir notamment Karim BENYEKHLEF, « Les glissements du droit à la vie privée. De Feydeau à Facebook : de la comédie de mœurs à l'économie des données », dans V. GAUTRAIS, C. RÉGIS et L. LARGENTÉ (dir.), *Mélanges Molinari*, Montréal, Éditions Thémis, 2018, 291-319).

277 Shoshana ZUBOFF, *L'Âge du capitalisme de surveillance*, Paris, Éditions Zulma, 2019.

souvent évoqué. Il concerne aussi bien les environnements transactionnels, comme les places de marché virtuelles, que les plateformes vouées au partage d'informations.

Définition d'hypertrucages. Les hypertrucages sont notamment des images de synthèse réalisées en mobilisant les technologies fondées sur l'intelligence artificielle. Les fausses informations sont créées pour manipuler l'opinion. L'illusion de vérité est totale. L'utilisateur ne peut à l'œil nu différencier le vrai du faux. Le document hypertruqué est fabriqué par codage informatique, sans pour autant être basé sur des faits réels et vérifiables. La réalité n'a pas besoin d'exister. Seule compte l'existence de contenus numériques diffusés qui sont destinés à être vus, écoutés et surtout « likés »!

Apprentissage profond. Ces outils fonctionnant grâce aux techniques d'apprentissage profond et de l'intelligence artificielle sont capables du meilleur et du pire. Ils peuvent servir aussi bien aux individus qui cherchent de bonne foi à se présenter sous un meilleur jour qu'aux fraudeurs et harceleurs se camouflant sous de fausses identités. Ces technologies sont mobilisées afin d'alimenter la propagande politique et guerrière. Elles rendent possible la diffusion de masse de documents volontairement falsifiés. C'est une grave menace pour l'intégrité des délibérations démocratiques.

Des fins légitimes ou illicites. Les dispositifs permettant de fabriquer des images et vidéos truqués peuvent servir des fins légitimes. Les films de fiction et les jeux vidéo utilisent abondamment ces capacités techniques. Les interdire purement et simplement n'est pas une avenue réaliste. Il faut plutôt sophistiquer les processus régulateurs voués à distinguer le vrai du faux. En soi l'utilisation de dispositifs afin de générer des faux ou des informations entièrement altérées par l'intelligence artificielle est au minimum assujettie aux lois générales[278]. Mais se pose la question de savoir si les intermédiaires qui sont en mesure de détecter les pratiques délétères ou risquées devraient être tenus à des obligations plus intenses.

2.2.1.4 Le harcèlement

Risques à visibiliser. L'étude réalisée par le Conseil du statut de la femme[279] documente le phénomène de l'hostilité en ligne qui vise de façon disproportionnée les femmes, notamment celles en position de pouvoir ou qui interviennent dans les espaces publics. Ces constats mettent en relief la nécessité de mieux reconnaître et visibiliser les risques associés à la diffusion de propos en ligne. Il y a des propos qui sont interdits par les lois, que ceux-ci soient prononcés sur la rue ou lancés sur un site Internet. Il en est ainsi de la diffusion de menaces, harcèlement, propos racistes, misogynes, homophobes ou transphobes. Le droit québécois considère l'injure et la diffusion non consentie d'images intimes comme des actes fautifs pouvant entraîner des recours civils. Mais comme le sens des mots et des images est tributaire de leur contexte de diffusion, plusieurs de ces règles sont difficiles à appliquer dans un environnement où l'information circule très vite. Cela pose le défi d'améliorer la capacité des instances judiciaires de distinguer rapidement entre le propos illégal de celui qui est de mauvais goût mais conforme aux lois.

---

278 *R.* c. *Larouche*, 2023 QCCQ 1853 (CanLII).

279 Conseil du statut de la femme, *Étude sur l'hostilité en ligne envers les femmes*, Québec, 2022, en ligne : <https://csf.gouv.qc.ca/article/2022/06/29/etude-sur-lhostilite-en-ligne-envers-les-femmes/>.

2.2.1.5 La publication non consensuelle d'images et d'images intimes

Puissance de diffusion. Les plateformes intermédiaires procurent à chacun des capacités de diffuser instantanément pratiquement toutes sortes d'informations, des sons, des images ou des textes. Il n'est pas étonnant que ces espaces aient pu donner lieu à la diffusion non consensuelle d'images, notamment des images intimes. Dans certaines provinces, des lois spécifiques ont été mises en place afin de procurer des recours aux victimes de publication non consensuelle d'images[280]. Par exemple, la Colombie Britannique s'est dotée d'un *Intimate Images Protection Act*[281]. Au Québec, l'article 28.1 de la *Loi sur la protection des renseignements personnels dans le secteur privé* prévoit un droit d'exiger la cessation de diffusion d'un renseignement personnel lorsqu'il est démontré que la diffusion du renseignement contrevient à la loi ou à une ordonnance judiciaire. Cette disposition paraît viser notamment des situations de partage non consensuel d'images intimes. Voilà une illustration des différences entre l'approche législative sectorielle et celle habituellement privilégiée au Québec d'édicter des lois ayant vocation à s'appliquer dans un vaste ensemble de situations présentes ou qui pourront se développer dans le futur.

2.2.1.6 La publicité et les influenceurs

Revoir les modes d'énonciation des réglementations. La publicité en ligne est l'une des activités la plus clairement visée par les lois québécoises, notamment celles portant sur la protection des consommateurs ou celle portant sur des activités ou produits réglementés. Mais les caractéristiques des environnements en ligne appellent à une réflexion sur les modes d'énonciation et d'application des réglementations relatives à la publicité au sens traditionnel ou aux modes nouveaux qui ont émergé en ligne. Par exemple, alors que la publicité destinée aux personnes de moins de treize ans est prohibée par la législation québécoise, des messages publicitaires ou de promotion destinés aux enfants circulent sur Internet, notamment par le truchement des activités d'entreprises ou d'individus comme les influenceurs. On s'inquiète des conséquences parfois néfastes des activités des influenceurs. On déplore souvent le fait que des activités de promotion et de publicité interdites dans d'autres contextes se trouvent à bénéficier d'un passe-droit lorsque ces pratiques sont le fait d'influenceurs actifs sur Internet.

2.2.1.7 Tendances persistantes

Trois tendances. Trois tendances demeurent pertinentes lorsqu'on examine les enjeux de responsabilité des intermédiaires. Dans les réseaux ouverts, comme Internet, il faut postuler l'impossibilité de contrôler ce à quoi accèdent les usagers. De même, on doit postuler que ce qui est illégal hors ligne ne saurait bénéficier d'une immunité une fois en ligne. Enfin, les intermédiaires ne peuvent être assimilés ou traités comme des éditeurs à l'égard des contenus ou des activités se déroulant dans leurs espaces.

---

280 *Intimate Images Protection Act*, RSNL 2018, c I-22, en ligne : <https://canlii.ca/t/53h6q>, *Intimate Images Unlawful Distribution Act*, SNB 2022, c1, en ligne : <https://canlii.ca/t/55ddz>, *Intimate Images and Cyber-protection Act,* SNS 2017, c 7, en ligne : <https://canlii.ca/t/53dcv>, *Intimate Images Protection Act*, SBC 2023, c 11, en ligne : <https://canlii.ca/t/55zjj>.

281 Voir *Intimate Images Protection Act*, SBC 2023, c 11, en ligne : <https://canlii.ca/t/55zjj>.

2.2.1.8 L'impossibilité de contrôler ce à quoi accèdent les usagers

Individu souverain. Sur Internet, l'usager a le loisir d'accéder à tout document se trouvant sur le réseau. *A priori*, il est difficile d'envisager des règles de droit au regard de ce à quoi peuvent accéder les individus. Cependant, les plateformes sont susceptibles d'être tenues à des obligations, notamment à l'égard des risques auxquels peuvent être exposés les individus.

2.2.1.9 Ce qui est illégal hors ligne ne devient pas légal du seul fait que l'activité se déroule en ligne

L'État de droit à risque. Il est théoriquement facile de convenir que ce qui est illégal hors d'Internet l'est aussi en ligne. C'est l'État de droit qui est mis à mal si on accepte que certains gestes ou comportements contraires à la loi en dehors d'Internet bénéficient d'une impunité pratique sur Internet. Mais le départage entre ce qui est prohibé par les lois et ce qui est protégé par la liberté d'expression[282] se révèle souvent une entreprise difficile. Par exemple, différencier ce qui relève de la critique légitime de ce qui constitue du propos haineux nécessite de considérer le contexte d'énonciation. Un tel départage procède habituellement d'une démarche fort éloignée de celle de certains groupes de pression qui peuvent trouver leur intérêt à entretenir la confusion entre le propos effectivement interdit par les lois et les critiques qu'ils aimeraient voir censurées. La posture de ces groupes de pression peut finir par devenir le combustible alimentant les arguments de ceux qui réprouvent *a priori* les initiatives étatiques afin d'assurer l'application des lois sur Internet.

Évaluer la licéité d'un contenu. Pour garantir que seuls les contenus visés par les lois seront supprimés des espaces en ligne, il faut que l'évaluation du caractère illégal des propos soit effectuée dans le cadre d'un processus indépendant. Il faut que les lois habilitent un juge à décider après avoir examiné les faits et entendu les parties impliquées. Sauf pour les contenus dont le caractère illégal saute aux yeux comme certains contenus de pornographie juvénile, il importe de garantir qu'un juge évalue avec célérité le bien-fondé d'une demande de retirer des images ou des textes d'un réseau social ou d'une autre plateforme en ligne.

L'impératif de célérité. La nature même du cyberespace où les informations voyagent de façon virale à la vitesse de la lumière impose d'agir vite. Si on ne parvient pas à assurer rapidement le respect des lois dans les environnements en ligne, c'est la légitimité même des lois visant à protéger la dignité des personnes qui est mise à mal. Il est normal de s'attendre à ce qu'un contenu illégal soit retiré rapidement. La mise en place des mesures destinées à faire en sorte que ce qui est interdit hors-ligne soit aussi interdit en ligne passe nécessairement par la mise à niveau des processus judiciaires. On ne peut s'attendre à ce que le public trouve acceptable que la suppression de contenus illégaux comme des images intimes mises en ligne au mépris du consentement de la personne concernée prenne des mois, voire des années.

---

[282] Pierre TRUDEL, « Discours haineux et propos choquants », (2017) *Le Devoir*, en ligne : <https://www.ledevoir.com/opinion/chroniques/491002/discours-haineux-et-propos-choquants>.

2.2.1.10 Les intermédiaires ne peuvent être assimilés à des éditeurs mais ils sont en position de connaître les risques et de les minimiser

Pas de contrôle éditorial. Les intermédiaires d'Internet ne peuvent être assimilés à des éditeurs. Ils n'ont ni l'intention ni la capacité d'exercer un contrôle éditorial. De plus, l'article 19.17 de *l'Accord Canada–États-Unis–Mexique (ACEUM) - Chapitre 19* [283] – interdit de traiter un fournisseur ou un utilisateur d'un service informatique interactif comme un fournisseur de contenu informatif pour déterminer la responsabilité en cas de préjudices liés aux renseignements stockés, traités, transmis, distribués ou mis à disposition par le service.

L'usager prend les décisions éditoriales. L'un des principaux traits caractéristiques des plateformes en ligne est justement d'habiliter l'ensemble des usagers à prendre des décisions éditoriales. Mais cela ne signifie pas que les intermédiaires n'ont pas de responsabilité. Comme ils valorisent les données générées par les activités en ligne, il paraît légitime de leur imputer des devoirs de précautions. C'est à ce titre que plusieurs législations envisagent de restructurer certains de leurs devoirs autour d'obligations d'identifier les risques et de prendre les mesures systémiques afin de les minimiser.

2.2.2 Réactions législatives

Identifier et gérer les risques. Les plateformes, dont les réseaux sociaux, profitent du trafic généré par les activités se déroulant en ligne. Les lois doivent être mises à niveau pour leur imposer des devoirs de diligence. Mais, à moins d'installer les intermédiaires dans un rôle de méga censeurs, il est irréaliste de les tenir *a priori* responsables des propos des usagers comme l'est un journal ou un radiodiffuseur. Cela explique que plusieurs états démocratiques ont mis en place des dispositions afin de baliser la responsabilité supportée par les intermédiaires[284]. On reconnaît de plus en plus que les modèles d'affaires consistant à générer des profits en monétisant le nombre de clics résultant de pratiques délétères en ligne doivent être conditionnés à des obligations de gérer sérieusement les risques que cela induit pour les personnes. La tendance qui commence à poindre dans les législations de plusieurs pays démocratiques est d'imposer aux intermédiaires des obligations d'identifier et de gérer les risques associés aux activités qu'ils autorisent dans leurs espaces.

2.2.2.1 Réactions législatives et responsabilité en général

Diversité des régimes de responsabilité. Dans plusieurs pays, des législations ont été mises en place afin de préciser les conditions de la responsabilité des intermédiaires. Les options retenues par les États vont de l'imposition d'un régime de responsabilité stricte aux plateformes intermédiaires à un régime leur procurant une large immunité. D'autres approches reposent sur des mécanismes de notification des contenus possiblement illégaux (notice and notice). Mais les

---

283 Accord Canada–États-Unis–Mexique (ACEUM) - Chapitre 19 - Commerce numérique, en ligne : <https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cusma-aceum/text-texte/19.aspx?lang=fra>.

284 Emily LAIDLAW, *Mapping Current and Emerging Models of Intermediary Liability,* (2019, juin), en ligne : SSRN: <https://ssrn.com/abstract=3574727> ou <http://dx.doi.org/10.2139/ssrn.3574727>.

approches retenues dans la *Directive européenne sur le commerce électronique*[285] de même que celles qui commandent d'instituer un régime de responsabilité procurant les équilibres compatibles avec les droits de la personne sont celles qui se rapprochent le plus des choix du législateur québécois. Mais les approches des lois sur la responsabilité des intermédiaires visent toutes, d'une manière ou d'une autre, à préciser leurs devoirs à l'égard des contenus mis en ligne par leurs usagers[286].

2.2.2.1.1 Les Principes de Manille sur la responsabilité des intermédiaires

Émanation de la société civile. Rédigés en 2015 par des groupes de la société civile du monde entier, les Principes de Manille[287] sur la responsabilité des intermédiaires identifient les garanties de base et de meilleures pratiques pour assurer la mise en place de règles assurant la protection des droits lorsque les intermédiaires sont mis en cause. Les principes sont fondés sur les instruments des droits de l'homme et d'autres cadres juridiques internationaux. Ils se déclinent comme suit :

- Principe I. Les intermédiaires devraient être protégés par la loi de toute responsabilité concernant le contenu de tiers;
- Principe II. Il ne faut pas exiger que le contenu soit restreint sans ordre d'une autorité judiciaire;
- Principe III. Les demandes de restrictions de contenu doivent être claires, sans ambiguïté et suivre une procédure régulière;
- Principe IV. Les lois et les ordonnances et pratiques de restriction de contenu doivent être conformes aux tests de nécessité et de proportionnalité;
- Principe V. Les lois et les politiques et pratiques de restriction de contenu doivent respecter une procédure régulière;
- Principe VI. La transparence et la responsabilité doivent être intégrées dans les lois et les politiques et pratiques de restriction du contenu.

À la vérité, ces principes viennent préciser, pour les intermédiaires d'Internet, ce qui est généralement tenu pour constituer les exigences fondamentales de l'État de droit. Il paraît certain que le droit québécois actuel est conforme à ces principes.

2.2.2.1.2 Les principes de l'UNESCO

Un énoncé de principes. L'UNESCO a mis de l'avant des Principes afin de préserver la liberté d'expression, l'accès à l'information et les autres droits fondamentaux dans le contexte de

---

285 *Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment le commerce électronique, dans le marché intérieur* (« Directive sur le commerce électronique »), JO L 178 du 17.7.2000.

286 Joris VAN HOBOKEN et Daphne KELLER, *Design Principles for Intermediary Liability Laws*, document de travail pour leTransatlantic High Level Working Group on Content Moderation Online and Freedom of Expression, October 8, 2019, en ligne : <https://fsi.stanford.edu/publication/design-principles-intermediary-liability-laws >.

287 « Principes de Manille sur la responsabilité des intermédiaires », (2015), en ligne : <https://www.eff.org/files/2015/10/31/manila_principles_1.0_fr.pdf>.

l'élaboration et de la mise en œuvre des processus de régulation des plateformes numériques[288]. Ils ont été établis dans le cadre d'un processus de consultation multipartite entrepris en septembre 2022. Ces principes visent à enrichir et à soutenir un espace mondial multipartite partagé pour débattre et partager de bonnes pratiques en matière de régulation des plateformes numériques; à servir d'outil à toutes les parties prenantes concernées pour plaider en faveur d'une régulation respectueuse des droits et pour identifier les responsabilités des gouvernements et des plateformes numériques. Les cinq principes renvoient à la mise en place de systèmes, de procédures et de reddition de comptes dans le cadre des processus de régulation.

Le premier principe énonce que les plateformes font preuve d'une diligence raisonnable en matière de droits de la personne et procèdent à des évaluations des risques en matière de droits fondamentaux. Celles-ci doivent être en mesure de démontrer aux régulateurs que leurs systèmes ou processus mis en place assurent une diligence raisonnable et continue en matière de droits de la personne, y compris les évaluations de l'impact sur les droits de la personne et les mesures d'atténuation. Les plateformes doivent procéder à des évaluations périodiques des risques afin d'identifier et de traiter tout dommage réel ou potentiel ou impact de leurs opérations sur les droits.

Le deuxième principe dispose que les plateformes doivent respecter les normes internationales en matière de droits de la personne, notamment en matière de conception de plateformes, de modération et de conservation des contenus. Elles doivent veiller à ce que les enjeux relatifs aux droits et à la régularité de la procédure soient intégrés à toutes les étapes du processus de conception et des politiques et pratiques de modération et de conservation de contenus. Les politiques de modération et de conservation de contenus doivent respecter les obligations des entreprises en matière de respect et de promotion des droits.

Sécurité par défaut. Les plateformes doivent intégrer les impératifs de sécurité dans leurs décisions lors de la conception de leurs environnements. Priorité doit être accordée à la sécurité des utilisateurs et à la création d'un environnement en ligne favorable à la participation au débat public. Les structures et procédures de modération et de conservation de contenus doivent être appliquées de manière cohérente et équitable.

Le troisième principe demande que les plateformes soient transparentes. Elles doivent rendre compte publiquement de la manière dont elles respectent les principes de transparence, d'explicabilité et d'information par rapport à ce qu'elles disent faire dans leurs conditions d'utilisation et leurs normes communautaires, y compris la façon dont elles ont répondu aux demandes d'information des autorités. La mise en œuvre de ce principe peut être modulée en fonction de la taille des plateformes. La régulation des plateformes numériques doit être transparente, aussi claire et concise que possible et aussi détaillée et complexe que nécessaire. La transparence ne se limite pas à la mise à disposition de textes juridiques ou d'une transmission de données; elle doit être comprise comme la fourniture aux parties prenantes des informations dont elles ont besoin pour prendre des décisions éclairées.

---

[288] UNESCO, « Préserver la liberté d'expression et l'accès à l'information : principes pour une approche multipartite dans le contexte de la régulation des plateformes numériques », version 3, (2023), en ligne : <https://unesdoc.unesco.org/ark:/48223/pf0000384031_fre>.

Transparence. L'efficacité des mécanismes de transparence des plateformes numériques doit faire l'objet d'une évaluation indépendante par rapport aux normes internationales au moyen d'évaluations qualitatives et empiriques quantitatives afin de déterminer si les informations fournies pour une transparence significative ont atteint leur objectif. De tels rapports doivent être régulièrement rendus publics.

Selon le quatrième principe, les plateformes doivent mettre des informations et des outils à la disposition des utilisateurs. Elles doivent prendre en compte l'impact de tout produit ou service sur le comportement des utilisateurs. Les plateformes doivent former leurs équipes de développement de produits à l'éducation aux médias et à l'information, y compris à la sécurité en ligne, dans une perspective d'autonomisation des utilisateurs, sur la base de normes internationales, et mettre en place des mécanismes de suivi et d'évaluation internes et indépendants.

Le cinquième principe concerne l'imputabilité. Il impose aux plateformes des obligations de rendre des comptes aux parties prenantes concernées. Elles doivent pouvoir démontrer que toute mesure prise lors de la modération et de la conservation de contenus a été menée conformément à leurs conditions d'utilisation et aux normes communautaires, et doivent rendre compte au système de régulation de manière équitable et précise des résultats obtenus au regard de leurs responsabilités. En cas de non-respect de cette disposition, les régulateurs doivent agir en conformité avec les Principes.

Obligations d'expliquer. Enfin, les plateformes numériques doivent être en mesure d'expliquer l'utilisation et l'impact des systèmes automatisés, y compris la mesure dans laquelle ces outils affectent la collecte de données, la publicité ciblée et la divulgation, la classification et/ou la suppression de contenus, y compris les contenus relatifs aux élections.

2.2.2.1.3 Le INFORM Consumer Act américain

Intégrité et équité. Aux États-Unis, le Congrès a adopté la loi sur l'intégrité, la notification et l'équité des marchés de détail en ligne pour les consommateurs – ou la loi INFORM Consumers[289]. Entrée en vigueur le 27 juin 2023, cette loi est appliquée par la Federal Trade Commission (FTC) et les États. Elle oblige les marchés en ligne, comme Amazon et eBay à vérifier et partager des informations sur les vendeurs tiers qui gèrent un volume élevé de transactions sur leurs plateformes dans le but de dissuader les acteurs malveillants de vendre des biens volés ou nuisibles.

Promouvoir la transparence. Lorsque les consommateurs achètent des produits sur des places de marché en ligne, l'identité du vendeur n'est souvent pas claire. L'objectif de la loi INFORM Consumers Act vise à promouvoir la transparence pour les transactions en ligne. Elle a aussi pour objectif de dissuader les criminels d'acquérir des articles volés, contrefaits ou dangereux et de les vendre sur les places de marché en ligne. La loi procure aussi aux utilisateurs du marché en ligne une possibilité de signaler les comportements suspects concernant les vendeurs tiers à volume élevé. La loi oblige les « marchés en ligne » au sein desquels des « vendeurs tiers à volume élevé » proposent des produits de consommation à collecter, vérifier et divulguer certaines informations sur ces vendeurs. La loi définit la notion de « vendeur tiers à volume élevé ». C'est un vendeur sur

---

289 *INFORM Consumers Act*, 15 U.S.C. § 45f, en ligne : <https://uscode.house.gov/view.xhtml>.

un marché en ligne qui, au cours de toute période continue de 12 mois au cours des 24 derniers mois, a eu sur cette plate-forme 200 ventes ou transactions distinctes ou plus de produits de consommation neufs ou inutilisés, et 5 000 $ ou plus de revenus bruts. Dans le calcul du nombre de ventes ou du montant des revenus bruts pour le seuil de « volume élevé » sur une place de marché en ligne donnée, les seules ventes considérées sont celles effectuées par l'intermédiaire de cette place de marché en ligne et pour lesquelles le paiement a été traité par la place de marché en ligne, soit directement ou via son processeur de paiement.

Marché en ligne. La loi définit un « marché en ligne » comme étant une personne ou une entreprise qui exploite une plate-forme destinée aux consommateurs qui permet à des vendeurs tiers de s'engager dans la « vente, l'achat, le paiement, le stockage, l'expédition ou la livraison d'un produit de consommation aux États-Unis ». La loi concerne les « produits de consommation », c'est à dire « un bien meuble corporel à vendre et qui est normalement utilisé à des fins personnelles, familiales ou domestiques ». Lorsqu'une entreprise répond à la définition d'un « marché en ligne », elle est tenue à certaines obligations. Les places de marché en ligne doivent collecter les informations de compte bancaire, les coordonnées et un numéro d'identification fiscale auprès des vendeurs tiers à volume élevé. En plus, elles doivent vérifier les informations qu'elles obtiennent des vendeurs tiers à volume élevé et exiger des vendeurs qu'ils maintiennent leurs informations à jour et qu'ils certifient leur exactitude au moins une fois par an. Pour les vendeurs tiers à volume élevé qui atteignent un certain niveau de ventes sur une plate-forme, les places de marché en ligne doivent divulguer dans les listes de produits ou les confirmations de commande des vendeurs des informations spécifiques sur le vendeur. Les places de marché en ligne doivent suspendre les vendeurs tiers à volume élevé qui ne fournissent pas les informations requises par la loi.

Signaler les comportements suspects. Enfin, les places de marché en ligne doivent fournir aux consommateurs, sur les listes de produits des vendeurs tiers à volume élevé, un moyen clair de signaler les comportements suspects.

2.2.2.1.4 La législation européenne sur les services numériques

Une législation d'avant-garde. La législation européenne sur les services numériques[290], à ce jour la plus avancée dans le monde occidental, prévoit d'obliger les plateformes à identifier et gérer les risques systémiques tels que la manipulation ou la désinformation. Avec l'entrée en vigueur de ces règles, les très grandes plateformes et les très grands moteurs de recherche seront obligés de prévenir l'utilisation abusive de leurs systèmes en adoptant des mesures pour évaluer les risques et en faisant réaliser des audits indépendants de leurs pratiques de gestion des risques[291].

Obligations d'information. Les règles européennes obligeront les plateformes à informer les utilisateurs, notamment sur les raisons pour lesquelles certaines informations leur sont recommandées. Les usagers auront le droit de se soustraire aux systèmes de recommandations

---

290 Voir en ligne : <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_fr#quelles-sont-les-prochaines-%C3%A9tapes>.

291 COMMISSION EUROPÉENNE, *Législation sur les services numériques: garantir un environnement en ligne sûr et responsable*, en ligne : <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_fr>.

fondés sur le profilage. De même, les utilisateurs pourront signaler facilement les contenus illicites et les plateformes devront traiter ces signalements avec diligence. Les données sensibles des utilisateurs telles que l'origine ethnique, les opinions politiques ou l'orientation sexuelle, ne pourront pas servir à sélectionner les publicités présentées.

Identifier les publicités. Les plateformes devront étiqueter toutes les publicités et informer sur l'identité de leurs promoteurs. Les plateformes devront fournir un résumé de leurs conditions générales aisément compréhensible et rédigé dans un langage clair, dans les langues des États où elles exercent leurs activités.

Protéger la vie privée. Les plateformes devront repenser leurs systèmes afin d'assurer un niveau élevé de protection de la vie privée et renforcer la sécurité des mineurs. Les publicités fondées sur un profilage s'adressant aux enfants ne seront plus autorisées. Des évaluations spéciales des risques, portant notamment sur les effets négatifs sur la santé mentale, devront être fournies à la Commission européenne. Les plateformes devront revoir la conception de leurs services, y compris leurs interfaces, systèmes de recommandations et conditions d'utilisation, afin d'atténuer les risques.

Traiter les risques de contenus illicites. Les plateformes et les moteurs de recherche auront l'obligation de prendre des mesures pour traiter les risques liés à la diffusion de contenus illicites en ligne et les effets négatifs sur la liberté d'expression et d'information. Elles devront avoir des conditions générales claires et les faire respecter avec diligence et de manière non arbitraire. Les plateformes devront aussi mettre en place un mécanisme permettant aux utilisateurs de signaler les contenus illicites et réagir promptement à ces signalements.

Analyser les risques spécifiques. Les plateformes auront l'obligation d'analyser les risques spécifiques aux activités qui s'y déroulent et mettre en place des mesures d'atténuation, par exemple pour empêcher la propagation de la désinformation et l'utilisation frauduleuse de leurs services.

Audits indépendants. Les plateformes devront se soumettre à un audit externe et indépendant leur évaluation des risques et les mesures qu'elles prennent pour assurer le respect de toutes les obligations découlant du règlement sur les services numériques. Elles devront rendre public le registre de toutes les publicités présentées sur leur interface. Les plateformes devront publier des rapports de transparence sur les décisions de modération des contenus et leurs opérations de gestion des risques.

2.2.2.1.5 La loi française sur les influenceurs en ligne

Lutter contre les dérives. La *Loi du 9 juin 2023 visant à encadrer l'influence commerciale et à lutter contre les dérives des influenceurs sur les réseaux sociaux*[292] définit et encadre l'activité des influenceurs sur les réseaux sociaux. Son objectif est de mieux lutter contre certaines dérives et arnaques constatées (incitation à faire des régimes alimentaires dangereux, de la chirurgie esthétique, des paris excessifs, promotion de contrefaçons...).

---

[292] Loi n° 2023-451 du 9 juin 2023 visant à encadrer l'influence commerciale et à lutter contre les dérives des influenceurs sur les réseaux sociaux (1) ELI, en ligne : <https://www.legifrance.gouv.fr/eli/loi/2023/6/9/ECOX2308125L/jo/texte>, Alias : <https://www.legifrance.gouv.fr/eli/loi/2023/6/9/2023-451/jo/texte> JORF n°0133 du 10 juin 2023.

Définition d'influenceur. La loi définit les influenceurs comme étant les personnes qui contre rémunération ou avantages en nature « mobilisent leur notoriété auprès de leur audience pour communiquer » en ligne « des contenus visant à faire la promotion, directement ou indirectement, de biens, de services ou d'une cause quelconque ». L'activité d'agent d'influenceurs, qui met ceux-ci en relation avec les marques, est également définie. Des mesures spécifiques protègent les enfants influenceurs.

Contrats écrits obligatoires. Au-delà d'un seuil de rémunération ou d'avantages en nature, la loi oblige les influenceurs, leurs agents et les annonceurs à conclure des contrats écrits comportant des clauses obligatoires comme les missions confiées, les conditions de rémunération, clause de soumission au droit français dès lors que sont visés des abonnés situés en France.

Responsabilité. Afin d'assurer l'indemnisation d'éventuelles victimes, la loi considère que l'annonceur, l'influenceur et son agent sont solidairement responsables. Les influenceurs résidant à l'étranger hors Europe devront désigner un représentant légal dans l'Union européenne et y souscrire une assurance civile dès lors qu'ils visent un public en France.

Publicité. Les influenceurs doivent respecter le cadre légal sur la publicité et la promotion des biens et des services. De plus, la loi interdit les publicités faisant la promotion de la chirurgie et la médecine esthétique; de certains produits et services financiers (notamment concernant les actifs numériques); de l'abstention thérapeutique; des sachets de nicotine (dont la vente sur Internet se développe auprès des adolescents); des abonnements à des conseils ou des pronostics sportifs, etc. La publicité impliquant des animaux sauvages est aussi interdite (sauf pour les zoos). La publicité des jeux d'argent et de hasard est encadrée afin de protéger les mineurs, de même que la promotion d'inscriptions à des formations professionnelles. Les influenceurs seront responsables vis-à-vis des acheteurs en cas de non-livraison, de produits contrefaits ou de piètre qualité.

2.2.2.1.6 Les propositions de groupes de réflexion

Protéger l'intégrité des échanges. De son côté, la *Commission canadienne de l'expression démocratique* a mis de l'avant un ensemble de propositions pour la mise en place de mécanismes destinés à protéger l'intégrité des échanges en ligne[293]. On y rappelle que les plateformes ne sont pas des diffuseurs neutres. Les plateformes structurent le contenu en fonction de leurs intérêts commerciaux. Elles doivent donc avoir une plus grande responsabilité pour les préjudices qu'elles se trouvent à amplifier ou à propager. La Commission propose d'imposer aux messageries et aux plateformes de réseaux sociaux un devoir légal d'agir de façon responsable. Cela vaudrait aussi pour les moteurs de recherche et d'autres opérateurs impliqués dans la circulation de contenus générés par les utilisateurs.

Superviser la gouvernance des plateformes. Pour assurer l'implantation de ces nouvelles obligations, un organisme public de réglementation serait habilité par la loi à superviser la gouvernance des plateformes. Il exercerait aussi une surveillance des activités de modération des contenus en tenant compte de la diversité des modèles d'interactions en ligne. Un tel organisme

---

293 Commission canadienne sur l'expression démocratique, *Diminuer un tort : un programme en six étapes pour protéger l'expression démocratique en ligne*, janvier 2021, en ligne : < https://ppforum.ca/fr/articles/diminuer-un-tort-un-programme-en-six-etapes-pour-proteger-lexpression-democratique-en-ligne/ >.

surveillerait les décisions relatives aux procédés (souvent automatisés) par lesquels les plateformes laissent circuler en ligne les sons, les textes et les images. Les décisions d'une telle instance réglementaire devront être fondées sur les lois et sujettes à un processus transparent de révision.

2.2.2.2 Réactions législatives et responsabilité en intelligence artificielle

Plusieurs énoncés de principe. Depuis que les technologies fondées sur l'intelligence artificielle de forme connexionniste commencent à être déployées, des nombreux énoncés de principe sont venus préciser les tenants et aboutissants des cadres législatifs destinés à en encadrer le déploiement. Par exemple, la *Déclaration de Montréal sur l'intelligence artificielle responsable* se décline en dix principes. On y affirme notamment que le développement et l'usage des systèmes d'IA doivent permettre d'accroître le bien-être de tous les êtres sensibles. Leur utilisation doit se faire dans le respect de l'autonomie des personnes et dans le respect de la vie privée. Les procédés fondés sur l'IA doivent aussi être compatibles avec les liens de solidarité entre les personnes et les générations. Ces systèmes doivent être soumis à l'examen et aux contrôles démocratiques. Ils doivent être compatibles avec la diversité sociale et culturelle. Leurs conséquences doivent être anticipées en fonction d'un principe de prudence. Le recours à de tels outils ne saurait avoir pour conséquence de déresponsabiliser les personnes qui y ont recours. À l'égard des utilisations de l'Intelligence artificielle et des autres procédés analogues, on observe une tendance à la mise en place d'obligations d'identification et de gestion des risques associés aux activités qui se déroulent sur les plateformes ou qui font usage de procédés d'IA.

Législations. Le projet de législation fédérale canadienne[294] et la législation européenne[295] se fondent sur des obligations faites aux entreprises qui déploient des systèmes d'IA d'identifier les risques et de mettre en œuvre les précautions conséquentes. De même, le projet européen segmente les obligations relatives aux systèmes d'intelligence artificielle en les distinguant selon les niveaux de risques qu'ils comportent.

2.2.3 Propositions

Vers un cadre élargi pour les intermédiaires. L'éclatement des problématiques mettant en cause la responsabilité des intermédiaires invite à s'interroger sur l'opportunité de modifier le droit québécois afin de répondre aux défis posés par les activités d'intermédiaires qui font beaucoup plus que simplement recevoir des documents émanant d'autrui. Des enjeux se posent au plan de la protection des libertés, de la maîtrise des risques de même que de l'opportunité d'identifier des devoirs plus spécifiques aux acteurs intermédiaires.

Préciser les critères relatifs à la connaissance. À l'égard de la responsabilité des intermédiaires, une approche possible consisterait à reconduire le régime actuellement prévu à l'article 22 de la

---

294 Projet de loi C-27 : *Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois*, juin 2022.

295 Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'union, com/2021/206 final.

LCCJTI mais en ajoutant des dispositions qui viendraient préciser les critères à considérer afin d'évaluer la connaissance de fait requise pour déclencher la responsabilité.

Nécessité de cyberjuges. La disponibilité d'instances capables d'instruire et de juger en ligne paraît s'imposer. Difficile d'ignorer que les décisions des différentes plateformes peuvent être l'objet de contestations par des usagers situés au Québec. Le rapport de la Commission canadienne de l'expression démocratique convient de la nécessité de cybertribunaux capables d'instruire avec célérité les conflits pouvant impliquer des usagers québécois et des entreprises qui y font affaire par Internet. Au fur et à mesure que se généralisent les activités en ligne, il paraît opportun de prévoir que les conflits nécessitant l'intervention d'un juge indépendant puissent être instruits en ligne.

Approche neutre ou spécifique ? Il importe de considérer la mise en place d'une instance ayant mandat d'assurer la conformité avec les conditions minimales qui seraient imposées pour le déploiement de certains dispositifs technologiques fondés sur l'intelligence artificielle. Dans les secteurs dotés d'instances de régulation, celles-ci devraient être en mesure d'intervenir en ligne lorsque cela est compatible avec le règlement efficace des conflits. Il apparaît en effet que le déploiement des technologies dans de multiples secteurs devraient être l'objet d'encadrements spécifiques. Par exemple, les conditions d'usage des véhicules autonomes devraient être énoncées dans les législations relatives au transport et à l'usage des espaces publics. De même, les règles sur la publicité dirigée vers les consommateurs devraient relever des instances chargées d'assurer la protection des consommateurs que leurs activités se déroulent en ligne ou ailleurs. Au sein de chacun de ces processus, seraient évaluées les mesures afin de protéger les droits fondamentaux dont la liberté d'attention, quels devoirs de diligence à l'égard de quels acteurs. De même, ces processus devraient assurer la mise en place de guides et de modèles d'évaluation des risques de même que des processus garantissant l'imputabilité algorithmique. Surtout, ces différentes instances, nécessairement publiques et privées, devraient fonctionner de façon concertée au sein de réseaux capables de suivre proactivement les évolutions et les différentes pratiques afin d'anticiper les tendances et les changements qui pourraient se révéler nécessaires dans les réglementations.

Un réseau de régulateurs. Les instances québécoises de régulation devraient être parties prenantes à des réseaux de régulateurs constitués à la fois d'entités publiques et de groupes de la société civile.

PROPOSITION #10 : À l'égard de la responsabilité des intermédiaires, une approche possible consisterait à reconduire le régime actuellement prévu à l'articles 22 de la LCCJTI, mais en ajoutant des dispositions qui viendraient préciser les critères à considérer afin d'évaluer la connaissance de fait requise pour déclencher la responsabilité.

Dans un deuxième temps, il importe de considérer la mise en place d'une instance ayant mandat d'assurer la conformité avec les conditions minimales qui seraient imposées pour le déploiement de certains dispositifs technologiques fondés sur l'intelligence artificielle. Si le Comité d'harmonisation pourrait jouer ce rôle de façon générale (voir le para. 1.2.3.2), il devra tenir compte de spécificités qui l'empêchent de traiter de certaines questions trop associées à un domaine en particulier (ex. : voitures autonomes, enseignement, etc.).

Une telle instance de régulation pourrait prendre la forme d'un réseau de régulateurs constitué à la fois d'entités publiques et de groupes de la société civile.

Dans les secteurs dotés d'instances de régulation, celles-ci devraient être en mesure d'intervenir en ligne lorsque cela est compatible avec le règlement efficace des conflits. Il apparaît en effet que le déploiement des technologies dans de multiples secteurs devraient être l'objet d'encadrements spécifiques.

2.2.3.1 Assurer la cohérence dans l'application des règles de droit

Assurer l'effectivité des lois. Le défi est d'assurer dans les espaces virtuels l'application effective des règles de droit qui prévalent dans les espaces physiques. Plusieurs espaces en ligne facilitent l'accomplissement de fonctions qui sont sujettes à des réglementations. Par exemple, la vente de médicaments en ligne tombe sous le coup des lois régissant la profession de pharmacien.

Des outils pour agir proactivement. Les intermédiaires ne pouvant devenir responsables qu'une fois qu'ils sont informés du caractère illicite d'une activité se déroulant sur leurs plateformes, il devient nécessaire d'assurer que les instances chargées d'appliquer les lois soient dotées des outils et ressources nécessaires pour identifier de possibles activités illicites se déroulant sur des plateformes fréquentées au Québec. Une telle capacité d'identifier les activités illicites suppose d'agir de façon proactive, sans attendre de plaintes qui pourraient ne jamais venir. Il sera en effet difficile à moyen terme de tolérer que des ordonnances de non-publication émises afin de protéger les enfants impliqués dans une affaire instruite devant un tribunal puissent être ignorées dès lors qu'une personne agit sur une plateforme de réseau social. Plusieurs activités de veille pourraient être organisées en favorisant la mise en synergie des instances publiques et des groupes associatifs, par exemple, les associations de défense des consommateurs ou de protection des enfants. Sans une politique résolument dirigée de manière à assurer que ce qui est prohibé par les lois, le soit aussi effectivement en ligne, c'est la confiance envers la règle de droit qui pourra être mise à mal.

PROPOSITION #11 : Les intermédiaires ne pouvant devenir responsables qu'une fois qu'ils sont informés du caractère illicite d'une activité se déroulant sur leurs plateformes, il devient nécessaire d'assurer que les instances chargées d'appliquer les lois soient dotées des outils et ressources nécessaires pour identifier de possibles activités illicites se déroulant sur des plateformes fréquentées au Québec. Une telle capacité d'identifier les activités illicites suppose d'agir de façon proactive, sans attendre de plaintes qui pourraient ne jamais venir. Mais plusieurs activités de veille pourraient être organisées en favorisant la mise en synergie des instances publiques et des groupes associatifs, par exemple, les associations de défense des consommateurs ou de protection des enfants.

2.2.3.2 Des régulations sectorielles fonctionnant en réseaux

Cloisonnements contreproductifs. Les situations se déroulant en ligne défient les catégories traditionnelles qui compartimentent les lois et les organismes publics. L'application des lois ne peut plus être bridée par les limites d'une vision compartimentée du droit héritée de l'époque où les réseaux constituaient l'exception. Pour avoir la capacité d'intervenir sur des réalités qui se déploient en réseau, il faut déployer des modes d'intervention qui fonctionneront en réseau. Par exemple, les instances chargées de la régulation de produits porteurs de hauts risques comme les médicaments fonctionnant en s'appuyant sur des réseaux de régulateurs et de laboratoires.

Cadre des plateformes. À cet égard, la mise en œuvre de la réglementation européenne imposant aux grandes plateformes d'identifier et de gérer les risques procure une opportunité pour le Québec. En introduisant dans la législation québécoise des obligations à la fois analogues à celles qui prévalent en Europe à l'égard des intermédiaires, le Québec se donne une capacité d'agir en réseau avec les régulateurs européens et pourra se trouver en position de bénéficier des mesures mises en place par ces derniers. Pour le moins, l'étude d'un article 22.1 semble nécessaire afin d'identifier les obligations qu'une plateforme doit avoir dès lors qu'elle dispose du contrôle des données des usagers. La notion de contrôle est en effet déterminante dans la LCCJTI pour identifier les différents cadres de responsabilité (notamment les art. 22, 26, 36, 37). Alors que l'article 22, justement, implique un contrôle *a posteriori* des données, c'est-à-dire après que l'intermédiaire a eu la connaissance d'une problématique, il importerait de prévoir une conservation avec un contrôle *a priori*, correspondant à la situation des plateformes actuelles. Une telle disposition devrait sans doute s'attacher à une définition de ce qu'est une plateforme; et notamment du cadre concernant les plus grandes ayant le potentiel de risques le plus conséquent. Une telle intervention législative serait en mesure d'étayer et préciser la portée des obligations qui doivent être déterminées dans la décision contre *Facebook* au sujet duquel la Cour d'appel a récemment autorisé un recours collectif[296].

PROPOSITION #12 : Il nous semble pertinent d'identifier dans une nouvelle disposition après l'article 22 un régime de responsabilité qui viendrait densifier les obligations à l'égard des plateformes.

2.2.3.3 Protéger la liberté d'attention

Une ressource précieuse. Dans l'environnement hyperconnecté où il est si facile de diffuser, même les pires mensonges, ce n'est plus la prise de parole qui est onéreuse. C'est plutôt l'attention des auditeurs qui constitue la ressource rare et précieuse. La capacité de manipuler l'attention est à la portée de beaucoup de monde. Sur Internet, la censure opère selon des logiques différentes de celles qui prévalaient lorsque l'imprimé ou la radiodiffusion étaient les médias dominants. Pour garantir l'effectivité de la liberté de s'exprimer et de débattre, il faut non seulement lutter contre la censure dans ses manifestations classiques, il faut aussi protéger contre la manipulation et assurer l'intégrité de l'attention de ceux qui écoutent.

Une liberté à protéger. Avec la généralisation des robots capables de produire à volonté de fausses images ou vidéos, la protection de la liberté effective de discuter et d'échanger des idées dans l'espace public requiert que les intermédiaires aient des obligations de détecter et éradiquer les pratiques déloyales et les usages frauduleux de leurs systèmes. Or, les plateformes intermédiaires sont susceptibles d'être le théâtre de manipulations et autres comportements trompeurs. La protection de la liberté d'attention des usagers pourrait constituer le fil conducteur de mesures imposant des devoirs aux plateformes.

---

296 *Beaulieu* c. *Facebook inc*., 2022 QCCA 1736.

PROPOSITION #13 : Protéger la liberté d'attention. Dans l'environnement hyperconnecté où il est si facile de diffuser, même les pires mensonges, ce n'est plus la prise de parole qui est onéreuse. C'est plutôt l'attention des auditeurs qui constitue la ressource rare et précieuse. La capacité de manipuler l'attention est à la portée de beaucoup de monde. Sur Internet, la censure opère selon des logiques différentes de celles qui prévalaient lorsque l'imprimé ou la radiodiffusion étaient les médias dominants. Pour garantir l'effectivité de la liberté de s'exprimer et de débattre, il faut non seulement lutter contre la censure dans ses manifestations classiques, il faut aussi protéger contre la manipulation et assurer l'intégrité de l'attention de ceux qui écoutent.

2.2.3.4 Des devoirs de diligence

Gestion diligente des risques. Les obligations imposées aux intermédiaires pourraient être structurées en fonction du risque que représente ce qu'elles font, jumelées à leur capacité d'agir. Par conséquent, la législation devrait formuler des attentes modulées en fonction de l'importance de la plateforme pour un niveau de risque donné. Il faudrait envisager d'interpréter l'obligation d'agir de manière responsable de manière renforcée lorsqu'il s'agit de plateformes ciblant des enfants ou des plateformes de contenu pour adultes. À plus forte raison, il faudrait formuler des obligations plus conséquentes lorsque la plateforme véhicule des contenus d'exploitation sexuelle des enfants, du partage non consensuel d'images intimes ou de la diffusion en direct d'une activité illicite.

2.2.3.5 Obligations d'évaluer et de gérer les risques

Risques à évaluer et à gérer. Le régime de responsabilité des intermédiaires devrait inclure une obligation pour les intermédiaires d'agir proactivement pour identifier et évaluer les risques associés aux activités qui se déroulent sur la plateforme. Mais il est essentiel de trouver le juste équilibre afin d'éviter que la gestion de risque soit appliquée au moyen d'exclusions arbitraires de certains contenus ou de certaines activités.

Identifier les risques. Chaque intermédiaire assujetti à la Loi serait tenu à une obligation d'identification des risques et aurait le devoir de démontrer qu'il prend des mesures raisonnables afin de gérer les risques. L'approche reconnaît que les risques peuvent varier selon les types de plateformes et les types de service. Les risques varient également en fonction des types d'activités qui peuvent se dérouler sur une plateforme. Par exemple, dans *Beaulieu* c. *Facebook*[297], la Cour d'appel convient de la nécessité de tenir compte de formes de discrimination occulte, indirecte et systémique, dont les victimes alléguées ne sont pas conscientes et qui peuvent engendrer des conséquences dommageables.

Principales phases de la gestion de risques. On peut représenter la gestion des risques en la déclinant en plusieurs étapes. Une démarche préliminaire, d'identification des risques pour les principaux acteurs concernés par les activités se déroulant sur une plateforme. L'identification préliminaire des risques permet d'identifier les mesures et précautions qui doivent être mises en place. En seconde étape, celle de l'observation en mode continu permet de valider l'évaluation préliminaire des risques. Tout au long du cycle d'observation et d'évaluation des risques,

---

[297] *Beaulieu* c. *Facebook inc*., 2022 QCCA 1736 (CanLII), en ligne : <https://canlii.ca/t/jtpzj>, 22 décembre 2022.

l'organisme de régulation reçoit les évaluations des risques de même que les rapports de suivi. L'organisme de régulation valide les mesures mises en place afin de gérer les risques et, le cas échéant, prescrit des mesures additionnelles.

Transparence. Les évaluations des risques sont rendues disponibles au public qui peut en prendre connaissance et introduire des observations. Cela peut donner lieu à un examen public sur les pratiques exemplaires et les possibles carences. L'analyse de risque est mise à jour en continu et peut faire l'objet de révision lorsqu'un changement significatif intervient dans le déroulement des activités prenant place sur la plateforme.

PROPOSITION #14 : Des devoirs de diligence pour les intermédiaires. Les obligations imposées aux intermédiaires pourraient être structurées en fonction du risque que représente ce qu'elles font, jumelées à leur capacité d'agir. Par conséquent, la législation devrait formuler des attentes modulées en fonction de l'importance de la plateforme pour un niveau de risque donné.

PROPOSITION #15 : Obligations d'évaluer et de gérer les risques. Le régime de responsabilité des intermédiaires devrait inclure une obligation pour les intermédiaires d'agir proactivement pour identifier et évaluer les risques associés aux activités qui se déroulent sur la plateforme. Mais il est essentiel de trouver le juste équilibre afin d'éviter que la gestion de risque soit appliquée au moyen d'exclusions arbitraires de certains contenus ou de certaines activités.

Chaque intermédiaire assujetti à la loi serait tenu à une obligation d'identification des risques et aurait le devoir de démontrer qu'il prend des mesures raisonnables afin de gérer les risques. L'approche reconnaît que les risques peuvent varier selon les types de plateformes et les types de services. Les risques varient également en fonction des types d'activités qui peuvent se dérouler sur une plateforme.

2.2.3.6 L'imputabilité algorithmique

Corollaire de l'obligation de gérer les risques. L'effectivité des devoirs d'évaluer et de gérer les risques suppose des garanties de vérification indépendante des processus techniques, au premier chef, les dispositifs fonctionnant au moyen d'algorithmes.

Mécanisme fondamental. Les algorithmes sont un mécanisme fondamental du fonctionnement du monde connecté. On ne peut en soi les interdire. Les algorithmes ont le potentiel de générer des décisions qui ont des conséquences bien réelles sur les personnes. Il faut se demander si leur usage ne doit pas être encadré par des processus crédibles de contrôle de la raisonnabilité des décisions qu'ils engendrent. Le cadre juridique québécois doit prendre la mesure des effets normatifs qu'ils engendrent. Il faut que les personnes concernées soient en mesure de savoir comment, sur quelles bases, sur quels présupposés fonctionnent les algorithmes; à partir de quels raisonnements ils génèrent leurs décisions. Par défaut, les algorithmes imposent leur logique et leur « loi », ils régulent le fonctionnement des objets et influent sur les comportements des personnes. En régulant les informations et les objets, les algorithmes régulent les comportements. Ces dispositifs automatisés peuvent rendre des activités possibles ou impossibles. Ils peuvent fixer les prix en temps réel selon différents paramètres, montrer ou cacher des messages. Les algorithmes font des calculs en temps réel pour déterminer quel message publicitaire sera affiché sur une page Web, quels biens de consommation seront proposés à l'internaute, quels contenus seront suggérés à

l'usager. À bien des égards, les algorithmes régissent les comportements autant, sinon plus, que le font les lois et règlements régissant les activités quotidiennes.

Transparence et imputabilité. Plusieurs estiment qu'il n'est pas réaliste d'assortir l'usage des algorithmes d'une obligation de transparence[298]. Certains ont plutôt préconisé que les lois étatiques instituent des processus de régulation inspirés de ceux qui régissent le développement et la mise en marché des médicaments et d'autres semblables produits complexes. Le développement et la mise en marché des médicaments sont soumis à des exigences quant à la validation des effets de ces produits, de leur efficacité et de leurs conséquences non prévues. Appliquer un tel modèle aux algorithmes impliquerait des obligations de partager les informations relatives au fonctionnement des outils fondés sur des algorithmes. Il faudrait également que les autorités publiques disposent d'une réelle capacité d'imposer des processus de vérification et de validation.

Conformité aux droits fondamentaux. Réguler les processus fondés sur des algorithmes, c'est obliger ceux qui les utilisent à garantir qu'ils fonctionnent en conformité avec les principes des lois étatiques et les droits fondamentaux. Cela suppose une capacité de vérification transparente pour le public. Si le monde connecté doit fonctionner dans le respect des principes démocratiques, il faudra rapidement penser un cadre régulateur à la mesure des enjeux que comportent les processus décisionnels fondés sur des procédés aussi puissants.

PROPOSITION #16 : L'effectivité des devoirs d'évaluer et de gérer les risques suppose des garanties de vérification indépendante des processus techniques, au premier chef, les dispositifs fonctionnant au moyen d'algorithmes.

2.3 LCCJTI + identité

Mise en contexte. Tel que le souligne la CNIL, « [d]ans le contexte de la protection des données, et plus largement dans celui des systèmes informatiques, l'identité correspond à un ensemble d'attributs associés à une personne physique qui permet de la relier à d'autres données »[299]. L'organisme poursuit en précisant que le concept d'identité renvoie à plusieurs notions distinctes, à savoir :

- l'identité propre en philosophie (ipséité) ou ce qui fait qu'une personne est unique et distincte d'une autre[300];
- l'identité personnelle, c'est-à-dire à la conscience et la représentation qu'une personne a d'elle-même;

---

298 Sylvia LU, « Data Privacy, Human Rights, and Algorithmic Opacity »,(2022) 110 *California Law Review*, en ligne : <https://ssrn.com/abstract=4004716>.

299 COMMISSION NATIONALE INFORMATIQUE ET DES LIBERTÉS, « L'identité numérique », (2023), en ligne : https://www.cnil.fr/sites/cnil/files/2023-03/CNIL_Dossier-thematique_Identite%20numerique.pdf, p. 4.

300 Notons que le principe de l'unicité est repris à l'article 4 de l'*Arrêté nº 2022-05 du ministre de la Cybersécurité et du Numérique en date du 26 août 2022* : « Unicité : Chaque personne est unique. L'unicité permet de distinguer une personne d'une autre et, selon le cas, de l'identifier de façon unique. Une personne détient par conséquent un seul compte pour elle-même et par système d'identification, sans possibilité de partager ou détenir ce compte avec une autre personne ».

- l'identité sociale, qui peut être multiple et se réfère au groupe, aux catégories sociales dont on possède des attributs[301].

C'est donc dire qu'une seule et même personne peut posséder plusieurs identités selon le contexte[302]. Juridiquement, les incidences de ces multiples identités sont contrôlées par le *Code civil du Québec*[303] dont l'article 5 prévoit que « [t]oute personne exerce ses droits civils sous le nom de famille et le prénom usuel qui lui sont attribués et qui sont énoncés dans son acte de naissance », alors que l'article 56 précise que « [c]elui qui utilise un autre nom que le sien est responsable de la confusion ou du préjudice qui peut en résulter ».

Avec l'adoption de la LCCJTI, le législateur québécois est venu compléter ce cadre juridique par l'ajout de dispositions visant non pas à réglementer le concept d'identité – tâche déjà assumée par le C.c.Q. – mais bien, par le biais des articles 40 à 45 et 47 à 62, à encadrer les mécanismes adoptés afin de valider l'identité d'individus dans un environnement numérique.

Identification et authentification. Or, cette validation de l'identité d'un individu passera nécessairement par deux mécanismes, à savoir : son identification et son authentification[304]. L'identification peut se définir comme étant l'« [o]pération qui consiste, pour une personne ou pour toute autre entité demandant l'accès au système informatique, à communiquer à ce dernier l'identité dont elle se réclame »[305], alors que l'authentification se résume à une « [p]rocédure de contrôle consistant à vérifier et à valider l'identité d'une entité qui fait une demande d'accès à un réseau, à un système informatique ou à un logiciel »[306]. On s'identifie pour se réclamer d'une identité et on s'authentifie pour la valider.

Par ailleurs, les questions d'identité ont été traitées dans la LCCJTI au regard de deux situations assez précises : d'une part, certaines dispositions abordent principalement les données biométriques (40 à 45) et, d'autre part, certaines traitent des questions en lien avec la certification (47 à 62),

---

301 COMMISSION NATIONALE INFORMATIQUE ET DES LIBERTÉS, « L'identité numérique », (2023), en ligne : <https://www.cnil.fr/sites/cnil/files/2023-03/CNIL_Dossier-thematique_Identite%20numerique.pdf>, p. 2.

302 COMMISSION NATIONALE INFORMATIQUE ET DES LIBERTÉS, « L'identité numérique », (2023), en ligne : <https://www.cnil.fr/sites/cnil/files/2023-03/CNIL_Dossier-thematique_Identite%20numerique.pdf>, p. 2.

303 RLRQ c CCQ-1991.

304 « Livre blanc sur l'identité numérique : Vivre à l'ère numérique en toute confiance, c'est possible », (2023), en ligne : <https://www.idlab.org/wp-content/uploads/2023/05/Vf_Livre_Blanc_IN_V6.3.pdf>, p. 5 et 6. Voir également l'article 1 de l'*Arrêté nº 2022-05 du ministre de la Cybersécurité et du Numérique en date du 26 août 2022*.

305 OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Grand dictionnaire terminologique*, « identification », (2001) en ligne : <https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/2074683/identification>. Voir à cette fin les articles 7 et 8 de l'*Arrêté nº 2022-05 du ministre de la Cybersécurité et du Numérique en date du 26 août 2022.*

306 OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Grand dictionnaire terminologique*, « authentification » (2019), en ligne : <https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/8374339/authentification>. Voir à cette fin les articles 9 à 11 de l'*Arrêté numéro 2022-05 du ministre de la Cybersécurité et du Numérique en date du 26 août 2022.*

notion intrinsèquement associée aux infrastructures à clé publique. Si cette approche s'inscrivait dans les tendances du moment, elle semble aujourd'hui dépassée à divers égards.

2.3.1 État des tendances

Plan. Une analyse de divers textes législatifs et de rapports relatifs à l'identification et l'authentification d'individus dans le cadre d'environnement numériques nous permet d'identifier trois principales tendances. La première (2.3.1.1) vient confirmer la position adoptée par le juge Easterbrook – à laquelle nous avons déjà fait référence – dans son désormais célèbre discours sur le « droit des chevaux » à l'effet que :

> « Beliefs lawyers hold about computers, and predictions they make about new technology, are highly likely to be false. This should make us hesitate to prescribe legal adaptations for cyberspace. The blind are not good trailblazers. »[307].

En effet, on constate un abandon des approches de validation des identités initiales et une abrogation des textes législatifs y associés. La seconde (2.3.1.2), découlant directement de la première, vise l'adoption de nouvelles approches agnostiques s'inscrivant dans la lignée du principe de neutralité technologique. Finalement, la troisième tendance observée (2.3.1.3) présente deux courants qui semblent être aux antipodes l'un de l'autre, mais qui sont pourtant parfaitement cohérents : d'une part l'adoption d'une identité numérique régalienne et, d'autre part, la multiplication des fournisseurs d'identité.

Finalement, nous nous permettrons certains commentaires relatifs à l'absence de tendance propre à certains nouveaux développements technologiques (2.3.1.4).

2.3.1.1 Tendance vers un abandon des approches initiales

2.3.1.1.1 Tendance vers un recul quant à la valorisation des signatures numériques

Infrastructures à clés publiques. À l'époque de l'adoption de la LCCJTI, l'une des principales tendances législatives relatives à l'identification des individus résidait dans la proposition d'un cadre juridique venant favoriser le recours aux infrastructures à clés publiques, notamment par l'adoption de dispositions propres aux certificats et aux signatures numériques. Pour rappel, la signature numérique est un « [p]rocédé cryptographique par lequel un bloc de données généralement chiffrées à l'aide d'un algorithme à clé publique est joint à un document électronique afin d'identifier son expéditeur, d'assurer l'intégrité des données et d'en garantir la non-

[307] Frank H. EASTERBROOK, « Cyberspace and the Law of the Horse », (1996) *University of Chicago Legal Forum* 207, 207.

répudiation »[308]. Ainsi, « on distingue la signature numérique de la signature électronique, qui est l'acte par lequel une personne exprime son consentement à l'aide d'un moyen électronique »[309].

Réglementation des signatures numériques. Cette tendance de légiférer autour de la signature numérique s'est d'abord observée aux États-Unis, où, dès 1995, l'Utah viendra adopter la *Utah Digital Signature Act*[310], reconnue comme étant la première loi en la matière au pays[311] Ce document législatif viendra par la suite inspirer les législateurs des autres états américains[312]. Suivront de près d'autres pays à travers le monde, dont la Corée du Sud avec l'adoption de sa *Digital Signature Act* (1999) et le Canada avec l'adoption de la *Loi sur la protection des renseignements personnels et les documents électroniques* (2000), dont l'article 31 prévoit la possibilité de recourir à une signature électronique dite « sécurisée » pour identifier un individu – laquelle signature doit résulter des opérations propres à une signature numérique[313].

En Europe, la Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques viendra instituer « un cadre juridique pour les signatures électroniques et certains services de certification afin de garantir le bon fonctionnement du marché intérieur »[314]. L'adoption de cette directive s'inscrivait notamment dans la suite du rapport intitulé « Assurer la sécurité et la confiance dans la communication électronique – Vers un cadre européen pour les signatures numériques et le chiffrement »[315] paru deux ans auparavant. Si la directive vient clairement favoriser le déploiement de signatures numériques, elle prévoit toutefois qu'une signature électronique ne peut être refusée du seul fait qu'elle n'est pas basée sur une technologie d'infrastructure à clé publique[316].

Mentionnons finalement que la *Commission des Nations Unies pour le droit commercial international* adoptera, en 2001, une *Loi type sur les signatures électroniques*. Comme la Directive européenne et la Loi canadienne, la Loi type vient promouvoir le recours aux signatures numériques sans pour autant écarter les autres formes de signatures[317].

---

308 OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Grand dictionnaire terminologique*, « signature numérique » (2022), en ligne : <https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/8384641/signature-numerique>.

309 OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Grand dictionnaire terminologique*, « signatur numérique » (2022), en ligne : <https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/8384641/signature-numerique>.

310 *Utah Code* §§ 46-3-101 to 46-3-504. Enacted by L. 1995, ch. 61.

311 R. Jason RICHARDS, « The Utah Digital Signature Act As "Model" Legislation : A Critical Analysis », (1999) 17 *J. Marshall J. Computer & Info. L.* 873, 875.

312 *Id.*.

313 *Règlement sur les signatures électroniques sécurisées*, DORS/2005-30, art. 2.

314 Article premier de la *Directive 1999/93/CE*.

315 COMMISSION EUROPÉENNE, « Assurer la sécurité et la confiance dans la communication électronique – Vers un cadre européen pour les signatures numériques et le chiffrement », (1998), en ligne : <https://op.europa.eu/fr/publication-detail/-/publication/015140f6-48c6-11ed-92ed-01aa75ed71a1/language-fr>.

316 Article 5(2) de la *Directive 1999/93/CE*.

317 Voir les articles 3 et 6 de la *Loi type de la CNUDCI sur les signatures électroniques*.

Abandon de l'approche. L'approche semble toutefois avoir perdu de sa pertinence, d'une part parce que la technologie propre aux infrastructures à clé publique, autrefois jugée universelle, ne pose que peu de questions de droit et présente sans doute un intérêt moindre du fait de solutions désormais diversifiées. D'autre part, son adoption ne s'est pas avérée aussi répandue qu'initialement anticipé[318]. D'ailleurs, la *Utah Digital Signature Act* est aujourd'hui surtout reconnue comme symbole des risques d'une adoption irréfléchie de lois visant à encadrer une nouvelle technologie dont on ne maîtrise pas la portée exacte. Pour preuve, le texte de loi a été aboli en 2006[319] parce que rarement utilisé[320] (notamment parce que la technologie proposée étaient désuète) et rendu caduc par l'adoption du *Uniform Electronic Transactions Act*[321], lequel encadre l'utilisation de signatures électroniques au sens large plutôt que la seule signature numérique[322]. Situation similaire en Corée du Sud où l'abrogation de la *Digital Signature Act* sera justifiée ainsi :

> « The government enacted the Digital Signature Law in 1999 and the Certified Certification Service the following year. Where legal bodies have been established that grant certificates proving the identity of the site online without documents, It obliged citizens to use them in financial transactions. Gradually, The presence of these certificates deepened to be used in real estate procurement, civil services, taxes, online shopping, and military service. However, the mandatory certifications hinder other services and technologies, The freedom of citizens to choose the means of electronic signature that suit them shall be restricted. It also needs to be renewed annually, and complex passwords that can be forgotten, and specific operating systems and browsers. These technical and service gaps are what prompted the government to abolish mandatory use in 2015. »[323]

En Europe, la tendance prendra plus de temps à s'imposer. En effet, si la Directive 1999/93/CE est abolie et remplacée par le Règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la Directive 1999/93/CE (dit règlement eIDAS) en 2014, la signature numérique demeurera un élément central dudit règlement eIDAS. Toutefois, la proposition de Règlement du Parlement européen et du Conseil modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique, exposé des motifs (eIDAS2) semble vouloir s'en éloigner.

---

318 Nicolas VERMEYS, « Fostering Trust and Confidence in Electronic Commerce », (2015) 20:2 *Lex-Electronica* 63, 79.

319 Repeal of Utah Digital Signature Act.

320 Anne BROACHE, « Utah May Erase Early but Unused E-Commerce Law », (2005) *Zdnet*, en ligne : <https://www.zdnet.com/article/utah-may-erase-early-but-unused-e-commerce-law/>.

321 Titre 46, chap. 4 du *Utah Code*.

322 Notons toutefois qu'au Canada, le projet de loi C-27, lequel viendrait notamment scinder la *Loi sur la protection des renseignements personnels et les documents électroniques* en deux textes distincts dont l'un serait intitulé « *Loi sur les documents électroniques* », ne propose pas de modifier les dispositions propres aux signatures électroniques sécurisées.

323 « South Korea Plans to Launch Digital Identity Based on Blockchain Technology », (2023), en ligne : <https://ibtekr.org/en/cases/south-korea-plans-to-launch-digital-identity-based-on-blockchain-technology/>.

Si le législateur québécois n'a pas choisi de légiférer expressément sur la signature numérique, l'article 39 de la LCCJTI précisant en effet que « [l]a signature peut être apposée au document au moyen de tout procédé qui permet de satisfaire aux exigences de l'article 2827 du *Code civil* », il n'en demeure pas moins que la section III de la LCCJTI réfère à la notion de certification – intimement liée à celle de signature numérique. D'ailleurs, conformément à ce qui s'observe notamment aux États-Unis, il n'est pas surprenant de constater que les articles 47 à 62 de la LCCJTI n'ont fait l'objet d'aucun traitement jurisprudentiel depuis l'entrée en vigueur de la Loi[324].

2.3.1.1.2 Tendance vers une reconfiguration de l'approche propre aux données biométriques

Approche québécoise. Avec l'adoption de dispositions propres aux données biométriques[325] et en accordant à la Commission d'accès à l'information le rôle d'autoriser et de superviser la mise en œuvre et l'utilisation de bases de données biométriques[326], le législateur québécois faisait en quelque sorte œuvre de pionnier puisque cette approche ne correspondait à aucun autre modèle législatif. Plus de vingt ans plus tard, on peut s'en féliciter.

D'ailleurs, à l'exception de la *Biometric Information Privacy Act* de l'Illinois[327] aucun texte législatif répertorié ne vient proposer un cadre propre à la protection des données biométriques. Soit, le considérant 53 du *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* (ci-après le RGPD) prévoit que : « [l]es États membres devraient être autorisés à maintenir ou à introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé », mais nos recherches n'ont débouché sur aucune tendance effective à cet effet.

Approche européenne. L'article 9 du RGPD vient plutôt simplement interdire l'utilisation de données biométriques pour identifier une personne sans son consentement[328]. Si une tendance peut

---

324 Selon une recherche effectuée via le moteur de recherche CanLII (<https://www.canlii.org/fr/>), le 15 septembre 2023.

325 Art. 43 et ss. LCCJTI.

326 Art. 45 LCCJTI.

327 740 ILCS 14. Notons toutefois que l'Illinois, comme une majorité d'états américains, ne possède pas de loi sur la protection des renseignements personnels et qu'elle se doit donc d'adopter des lois sectorielles. Par ailleurs, la loi ne prévoit aucun mécanisme similaire à celui proposé par la LCCJTI.

328 Notons que ce principe souffre cependant d'une série d'exceptions énoncées à l'article 9 RGPD, à savoir : le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale, dans la mesure où ce traitement est autorisé par le droit de l'Union, par le droit d'un État membre ou par une convention collective conclue en vertu du droit d'un État membre qui prévoit des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée; le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement; le traitement est effectué, dans le cadre de leurs activités légitimes et moyennant les garanties appropriées, par une fondation, une association

être identifiée, c'est donc celle d'autoriser[329] – voire de faciliter[330] – l'utilisation de données biométriques afin d'identifier et/ou d'authentifier un individu, sous réserve d'obtenir un consentement libre et éclairé. Pour ce faire, la CNIL propose une approche similaire à celle prévue à l'article 43 LCCJTI, à savoir :

> « La biométrie étant un traitement sensible, la CNIL préconise que **tout MIE l'utilisant propose une alternative équivalente pour accéder aux mêmes services**. Cela permet, d'assurer le **consentement libre** de l'usager. Cette solution alternative pourrait notamment prendre la forme d'un face-à-face (tel qu'un déplacement en préfecture, en mairie, ou auprès d'un autre service public accueillant directement le public). »[331]

Ceci nous appert difficilement praticable en l'occurrence et – surtout – ne cadre pas avec ce qui est indiqué à l'article 9 RGPD. À cet égard, il importe de mentionner que l'article 43 al.2 LCCJTI est d'une rare rigueur, ayant pour effet d'empêcher l'utilisation de technologie « qui permet de savoir où [une personne] se trouve ». Dans les faits cela voudrait dire que les usagers de « mouchards » notamment dans l'industrie du transport sont systématiquement illégaux. Même si la disposition

---

ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale, à condition que ledit traitement se rapporte exclusivement aux membres ou aux anciens membres dudit organisme ou aux personnes entretenant avec celui-ci des contacts réguliers en liaison avec ses finalités et que les données à caractère personnel ne soient pas communiquées en dehors de cet organisme sans le consentement des personnes concernées; le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée; le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle; le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un 'État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée; le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé et soumis aux conditions et garanties visées au paragraphe 3; le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel; le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, conformément à l'article 89, paragraphe 1, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.

329 RGPD, art. 9. Voir également, COMMISSION NATIONALE INFORMATIQUE ET DES LIBERTÉS, « L'identité numérique », (2023), en ligne : <https://www.cnil.fr/sites/cnil/files/2023-03/CNIL_Dossier-thematique_Identite%20numerique.pdf>, p. 5.

330 *Digital Signature Act*, art. 6(1) (Corée du Sud), en ligne : <https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=55068&type=part&key=43>.

331 COMMISSION NATIONALE INFORMATIQUE ET DES LIBERTÉS, « L'identité numérique », (2023) en ligne : <https://www.cnil.fr/sites/cnil/files/2023-03/CNIL_Dossier-thematique_Identite%20numerique.pdf>, p. 5.

est difficile à appliquer, une rare jurisprudence trouve néanmoins le moyen de légaliser l'usage d'une pareille technologie[332].

Sinon, notons que cette tendance ne s'oppose pas à l'approche québécoise. Il est toutefois intéressant de souligner que les dispositions propres aux données biométriques se retrouvent au sein de textes propres aux données personnelles plutôt que de textes propres à l'identité numérique. Par exemple, la proposition de *Règlement du Parlement européen et du Conseil modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique, exposé des motifs* (ci-après : eIDAS2) ne mentionne les données biométriques qu'à un endroit dans ses considérants pour simplement souligner l'importance d'en assurer la protection et effectuer un renvoi à l'article 9 du RGPD.

L'approche québécoise demeure donc compatible avec ces tendances, même s'il reste 1) à vérifier son application à des situations nouvelles (comme les caméras dites intelligentes); 2) à valider si ces questionnements ne se présentent pas en porte-à-faux avec les règles applicables en matière de vie privée; et 3) à identifier si les dispositions en cause sont en accord avec les technologies actuelles.

2.3.1.2 Tendance vers l'adoption d'une approche agnostique

Neutralité technologique. Plutôt que de miser sur des technologies précises telles que les infrastructures à clé publique ou l'utilisation de données biométriques pour confirmer l'identité d'individus, on peut observer une migration vers une approche s'inscrivant dans la lignée du concept de neutralité technologique. Cette tendance s'observait déjà au sein des instruments normatifs européens et internationaux qui abordent – au même titre que les articles 2827 C.c.Q. et 39 LCCJTI – la notion de signature selon ses fonctions (identification d'un individu, lien avec le document et manifestation du consentement). Pour ne reprendre que cet exemple, l'article premier de la *Digital Signature Act* sud-coréenne définit la notion de signature électronique comme signifiant « data in electronic form which are attached to or logically associated with an electronic document […] to identify the signatory [and] To verify the fact that the electronic document has been signed by the signatory »[333].

Authentification multifacteur. Cette approche technologiquement agnostique s'est toutefois accentuée au cours des dernières années avec une valorisation du concept d'authentification multifacteur, soit un mode d'authentification qui met en œuvre, de façon concomitante, des procédés de vérification faisant appel à au moins deux facteurs d'authentification différents[334]. Par

---

332 Travailleuses et travailleurs unis de l'alimentation et du commerce, section locale 501 et Provigo Distribution inc. (Centre de distribution St-François), (Alain Carrière), 2009 QCSAT 94074.

333 *Digital Signature Act*, art. 1 (Corée du Sud), en ligne : <https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=55068&type=part&key=43>.

334 OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Grand dictionnaire terminologique*, « authentification multifacteur » (2022), en ligne : <https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/26557505/authentification-multifacteur>. Voir également l'*Arrêté nº 2022-05 du ministre de la Cybersécurité et du Numérique en date du 26 août 2022*, article 2 : 5° « authentification multifacteur : l'authentification de base ou avancée qui met en œuvre, de façon concomitante, au moins deux facteurs d'authentification distincts constituant une méthode d'authentification forte ».

exemple, l'annonce, en 2022, de l'adoption d'une architecture à vérification systématique[335] (Zero Trust Architecture) par le gouvernement américain place l'identification multifacteur au centre de la stratégie proposée par la Maison blanche :

> « This strategy places significant emphasis on stronger enterprise identity and access controls, including multi-factor authentication (MFA). Without secure, enterprise-managed identity systems, adversaries can take over user accounts and gain a foothold in an agency to steal data or launch attacks. This strategy sets a new baseline for access controls across the Government that prioritizes defense against sophisticated phishing, and directs agencies to consolidate identity systems so that protections and monitoring can be consistently applied. Tightening access controls will require agencies to leverage data from different sources to make intelligent decisions, such as analyzing device and user information to assess the security posture of all activity on agency systems. »[336]

Notons que cette approche d'authentification multifacteur a également été adoptée comme mécanisme d'identification et d'authentification par le Gouvernement du Canada[337] et divers services gouvernementaux québécois[338]. Elle est également favorisée par l'industrie et par les institutions financières[339].

Une éventuelle adoption plus généralisée de cette approche ne requiert toutefois aucun ajustement législatif, l'article 40 LCCJTI prévoyant déjà que « La vérification de l'identité d'une personne peut aussi être effectuée à partir de caractéristiques, connaissances ou objets qu'elle présente ou possède » sans par ailleurs indiquer que ces modes de vérification de l'identité ne peuvent s'additionner.

2.3.1.3 Tendance vers une approche à la fois plus centralisée et décentralisée

Plan. Si l'intitulé qui précède peut sembler incohérent, il représente néanmoins une tendance observable visant, d'une part, à mettre sur pied une identité « régalienne » unique pour interagir avec l'État et ses démembrements (2.3.1.3.1) et, d'autre part, à favoriser la multiplication des fournisseurs d'identité (2.3.1.3.2).

---

335 « Modèle de sécurité par lequel tous les usagers, programmes ou systèmes qui tentent de se connecter au réseau d'une organisation doivent être systématiquement authentifiés et autorisés ». Voir : OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Grand dictionnaire terminologique*, « modèle à vérification systématique » (2022), en ligne : <https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/26557550/modele-a-verification-systematique>.

336 EXECUTIVE OFFICE OF THE PRESIDENT AND OFFICE OF MANAGEMENT AND BUDGET, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, (2022, janvier), en ligne : <https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf>.

337 AGENCE DU REVENU DU CANADA, *Authentification multifacteur pour accéder aux services d'ouverture de session de l'ARC*, (2023, juillet), en ligne : <https://www.canada.ca/fr/agence-revenu/services/services-electroniques/services-ouverture-session-arc/authentification-multifacteur-acceder-services-d-ouverture-session-agence.html>.

338 Voir par exemple, ÉPARGNE PLACEMENTS QUÉBEC, *Transactions en direct*, en ligne : <https://transactions.epq.gouv.qc.ca/Client/AuthnConfigMultiFacteurs#_>.

339 « Livre blanc sur l'identité numérique : Vivre à l'ère numérique en toute confiance, c'est possible », (2023), en ligne : <https://www.idlab.org/wp-content/uploads/2023/05/Vf_Livre_Blanc_IN_V6.3.pdf>, p. 6.

En effet, comme le souligne la CNIL :

> « Une distinction peut être faite entre une identité « régalienne », reliée à l'état civil de l'individu et qu'il utiliserait dans ses démarches administratives ou formelles, et une identité « non régalienne », qu'elle soit reliée à un pseudonyme qu'il pourrait utiliser par exemple sur un site de rencontres, ou à un nom et un prénom d'usage (même reconnus par l'État) qu'il pourrait utiliser pour acheter un objet en ligne. »[340]

2.3.1.3.1 Tendance vers l'adoption d'une identité numérique régalienne

Identité numérique. Tel que nous y avons déjà fait référence, en 2014, en réaction (notamment) à « un relatif constat d'échec de la Directive 1999/93/CE sur la signature électronique »[341], les législateurs européens ont procédé à l'adoption du *Règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE*. Ce règlement visait notamment l'harmonisation des « moyens d'identification électronique utilisés dans l'Union européenne, afin qu'un usager dans un État membre puisse accéder aux services publics d'un autre État membre »[342]. Bref, il prévoit notamment – en ce qui nous intéresse – la création d'une identité numérique, soit « l'ensemble des données d'identification d'une personne physique ou morale et constituée notamment d'identifiants numériques permettant de la représenter de manière univoque »[343] fournie par les États membres. En effet, « les identités numériques ont […] pour particularité d'opérer un lien numérique entre différentes formes d'identités administratives ou caractérisées par les sciences sociales »[344] et repose sur « un élément matériel et/ou immatériel contenant des données d'identification personnelle et utilisé pour

---

340 COMMISSION NATIONALE INFORMATIQUE ET DES LIBERTÉS, « L'identité numérique », (2023) en ligne : <https://www.cnil.fr/sites/cnil/files/2023-03/CNIL_Dossier-thematique_Identite%20numerique.pdf>, p. 2.

341 AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION, *Le règlement EIDAS*, en ligne : <https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-reglement-eidas/#:~:text=Le%20r%C3%A8glement%20eIDAS%20s'applique,march%C3%A9%20de%20la%20confiance%20num%C3%A9rique>.

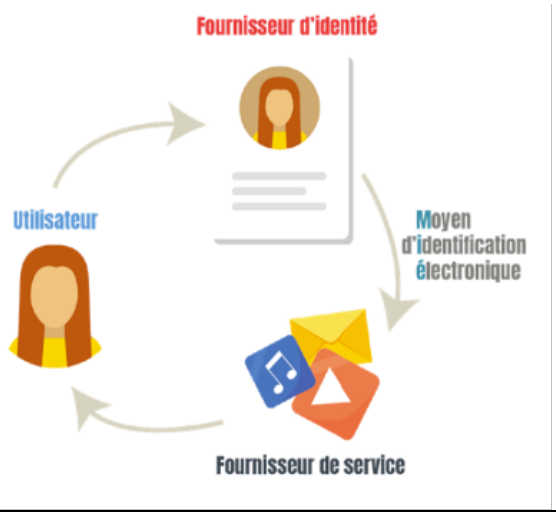
342 COMMISSION NATIONALE INFORMATIQUE ET DES LIBERTÉS, « L'identité numérique », (2023), en ligne : <https://www.cnil.fr/sites/cnil/files/2023-03/CNIL_Dossier-thematique_Identite%20numerique.pdf>, p. 5.

343 Benjamin ALI ABOUDOU *et al.*, « Guide d'encadrement sécuritaire de l'identité numérique », (2022), en ligne : <https://gric.recherche.usherbrooke.ca/wp-content/uploads/2022/04/guide_encadrement_securitaire_identite_numerique.pdf>. Les auteurs précisent par ailleurs que « [c]ette définition est inspirée de l'article 2 de la Loi n° 1.483 du 17 décembre 2019 relative à l'identité numérique de la Principauté de Monaco (voir *Journal de Monaco*, 27 déc. 2019. p. 3870). Cependant, il n'existe pas de consensus, ni en recherche et ni juridiquement, sur la nature exacte de l'identité numérique ».

344 COMMISSION NATIONALE INFORMATIQUE ET DES LIBERTÉS, « L'identité numérique », (2023) en ligne : <https://www.cnil.fr/sites/cnil/files/2023-03/CNIL_Dossier-thematique_Identite%20numerique.pdf>, p. 2.

s'authentifier à un service en ligne ».[345] Notons toutefois que les identités numériques ne sont pas propres aux personnes physiques; une personne morale pouvant également posséder une telle identité.

En soi, l'identité numérique vise en fait à « recréer un triangle de confiance dans l'espace numérique »[346] et de s'éloigner du modèle existant d'identification/authentification en silo, fragmenté et peu efficace.

Modèle actuel[347]	Identité numérique[348]
	

Comme on peut le constater, l'approche vient reproduire un modèle tripartite entre :

- **l'utilisateur** : une personne souhaitant accéder à un ensemble de services;
- **le fournisseur d'identité** : un tiers de confiance qui vient garantir les attributs présentés par l'utilisateur ainsi que le lien entre les attributs et cet utilisateur;

---

345 COMMISSION NATIONALE INFORMATIQUE ET DES LIBERTÉS, « L'identité numérique », (2023) en ligne : <https://www.cnil.fr/sites/cnil/files/2023-03/CNIL_Dossier-thematique_Identite%20numerique.pdf>, p. 4. Notons que l'identifiant utilisé variera selon le type de service auquel l'on désire avoir accès. Par exemple, le règlement eIDAS prévoit trois niveaux : un niveau de garantie « faible », lequel correspond à une vérification préalable succincte avec une authentification simple; un niveau « substantiel » pour les vérifications intermédiaires; et un niveau « élevé », qui garantit une vérification en profondeur et requiert une authentification forte. CNIL, p. 5.

346 « Livre blanc sur l'identité numérique : Vivre à l'ère numérique en toute confiance, c'est possible », (2023), en ligne : <https://www.idlab.org/wp-content/uploads/2023/05/Vf_Livre_Blanc_IN_V6.3.pdf>, p. 7.

347 Consult HYPERION, *L'impact économique de l'identité numérique au Canada : comprendre les avantages économiques considérables que cela peut apporter et le cout de l'inaction*, en ligne : <https://diacc.ca/wp-content/uploads/2021/05/Limpact-e%CC%81conomique-de-lidentite%CC%81-nume%CC%81rique-au-Canada_White-Paper.pdf>.

348 COMMISSION NATIONALE INFORMATIQUE ET DES LIBERTÉS, « L'identité numérique », (2023) en ligne : <https://www.cnil.fr/sites/cnil/files/2023-03/CNIL_Dossier-thematique_Identite%20numerique.pdf>, p. 4.

- **le fournisseur de service** : un opérateur qui met à la disposition de l'utilisateur un ensemble de services dont l'accès est conditionné soit à une authentification soit à une preuve d'attribut[349].

À certains égards, ce rapport tripartite se retrouve aussi dans la récente norme canadienne CAN/DGSI 103-1:2023[350], entre le sujet, l'émetteur et le vérificateur. Seulement, dans ce texte, il ne semble pas y avoir le même rapport à l'État qui joue un rôle plus grand, notamment à l'étape de l'émission des attributs d'identité.

Référence à des normes. Cette approche repose par ailleurs sur une autre tendance identifiée tout au long de la présente étude, soit celle de la délégation à des tiers en s'appuyant sur des normes, en l'occurrence, pour le Règlement eIDAS, les normes ETSI (European Telecommunications Standards Institute) et CEN (Comité Européen de normalisation)[351].

Courant international. La tendance engendrée par l'adoption du Règlement eIDAS, puis sa révision annoncée par le Règlement eIDAS2, s'est vue cristallisée avec le lancement récent des travaux du consortium POTENTIAL, lequel « a pour objectif de tester le déploiement d'un portefeuille d'identité numérique permettant de simplifier et sécuriser les démarches en ligne des citoyens européens, de faciliter le traitement des démarches par les services de l'administration et de lutter contre l'usurpation d'identité »[352].

---

349 *Id.*

350 CAN/DGSI 103-1:2023, seconde édition, Confiance et identité numérique – Partie 1 : notions fondamentales, 2023-04, en ligne : <https://dgc-cgn.org/>.

351 Voir le Mandat M/460.

352 MINISTÈRE DE L'INTÉRIEUR ET DES OUTRE-MER, *Lancement du consortium européen POTENTIAL pour l'identité numérique*, (2023, juillet), en ligne : <https://www.interieur.gouv.fr/actualites/communiques-de-presse/lancement-du-consortium-europeen-potential-pour-lidentite>. Parmi les services visés, mentionnons : l'accès aux services publics électroniques permettant aux citoyens de prouver leur identité sur les services gouvernementaux en ligne en vue de favoriser et simplifier leurs démarches administratives en ligne; l'ouverture de compte bancaire courant, d'épargne, et dépositaire en ligne visant à sécuriser l'identification des citoyens au moment des démarches et favoriser la lutte contre la fraude bancaire; l'enregistrement de carte SIM permettant aux citoyens de prouver leur identité au moment de l'ouverture d'une ligne téléphonique; le développement d'un « compagnon numérique » du permis de conduire sur un téléphone portable qui constitue une preuve du droit à conduire pouvant être utilisée par les forces de sûreté intérieure et par les agences de location de voiture; la signature électronique qualifiée à distance pour des contrats qui requièrent une preuve d'identité renforçant ainsi les dispositifs de lutte contre la fraude; la prescription médicale électronique qui permet aux usagers d'accéder à leurs données médicales et d'autoriser un accès à leurs données de prescriptions médicales aux personnels habilités.

Cette tendance, également suivie au Canada[353] et, évidemment, au Québec[354] est notamment appuyée par la Banque mondiale[355] et les Nations Unies[356]. Même aux États-Unis, où l'approche régalienne est historiquement mal perçue[357], un projet de loi intitulé « A Bill to establish a Government-wide approach to improving digital identity, and for other purposes » (ci-après : le « Improving Digital Identity Act of 2023 ») est présentement sous étude par le Congrès. La genèse de ce projet découle d'une demande de la « Commission on Enhancing National Cybersecurity » de procéder à la création d'un groupe de travail chargé de trouver des moyens de permettre aux agences gouvernementales de servir de source autorisée pour valider les attributs d'identité des citoyens américains[358]. Selon ce qui est indiqué au projet de loi, cette action permettrait aux agences gouvernementales et au secteur privé d'éliminer les risques importants liés à l'accès à divers services en ligne[359]. Le projet de loi part d'une série de constats dont certains nous apparaissent comme étant universels, à savoir :

- l'absence de moyens faciles, abordables, fiables et sûrs pour les organisations, les entreprises et les agences gouvernementales d'identifier si une personne est bien qui elle prétend être sur Internet génère des risques et nuit au commerce;
- les entités gouvernementales sont particulièrement bien positionnées pour fournir des composantes essentielles afin de combler les lacunes de l'infrastructure d'identité numérique et de renforcer les solutions d'identité et d'authentification numériques du secteur privé;
- les autorités étatiques sont particulièrement bien positionnées pour jouer un rôle dans l'amélioration des solutions d'identité numérique utilisées par les secteurs public et privé, vu leur rôle d'émetteurs de permis de conduire et autres documents d'identité couramment utilisés[360].

---

353 SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, *Une vision de l'identité du Canada digne de confiance* [vidéo], en ligne sur YouTube : <https://youtu.be/K7qtNvabX3c>. Voir également la Norme nationale du Canada CAN/DGSI 103-1:2023. Notons que le territoire du Yukon a déjà procédé, en 2022, à l'adoption d'un *Règlement sur l'identification numérique*, YD 2022/164.

354 GOUVERNEMENT DU QUÉBEC, *Programme Service québécois d'identité numérique*, (2023, septembre), en ligne : <https://www.quebec.ca/gouvernement/identite-numerique/programme-service-quebecois-identite-numerique#c144628>.

355 WORLD BANK, *Principes sur l'identification pour le développement durable : vers l'ère numérique*. (2021, février), en ligne : <https://documents1.worldbank.org/curated/en/470971616532207747/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf>.

356 C. HANDFORTH, K. LE, (2022, 19 mai), *Comment le numérique peut-il combler le « fossé identitaire » ?*, UNPD Blog, en ligne : <https://www.undp.org/fr/blog/comment-le-num%C3%A9rique-peut-il-combler-le-%C2%AB-foss%C3%A9-identitaire-%C2%BB>.

357 ACRONIS, *Data Sovereignty Around the World: Exploring Regulations in Canada, U.S., U.K., E.U., Brazil and Japan*, en ligne : <https://dl.acronis.com/u/rc/White-Paper-Acronis-Cyber-Protect-Cloud-Data-Sovereignty-Around-the-World-EN-US.pdf>.

358 *Improving Digital Identity Act of 2023*, art. 2.

359 *Id.*

360 *Id.*

2.3.1.3.2 Tendance vers une multiplication des fournisseurs d'identité

Partenariats public-privés. Si l'approche régalienne semble s'imposer, il importe de mentionner qu'elle présente déjà certaines failles. Ainsi, aux États-Unis l'*Improving Digital Identity Act of 2023* favorise un partenariat public-privé plutôt qu'une approche purement régalienne comme celle adoptée par le Yukon[361], par exemple. En effet, le projet de loi américain prévoit que :

> « The public and private sectors should collaborate to deliver solutions that promote confidence, privacy, choice, equity, accessibility, and innovation. The private sector drives much of the innovation around digital identity in the United States and has an important role to play in delivering digital identity solutions. »[362]

Même son de cloche en Corée du Sud où la Loi prévoyait déjà l'adoption de projets pilotes pour promouvoir la création et l'utilisation de diverses solutions d'identification/authentification[363]. Cette approche n'a été que réaffirmée avec l'abolition de l'usage exclusif de certificats accrédités en 2020 pour promouvoir l'utilisation de nouveaux mécanismes d'identification/authentification fiables dont le recours aux chaînes de blocs (voir la section 2.3.1.4.1), le tout afin de stimuler un niveau de confiance plus important dans le secteur des identifiants numériques[364]. En effet :

> « Since the abolition of mandatory accredited certificates, the government has granted legal authority to many electronic signature methods. Citizens can now prove their identity using their mobile phone number, bank account or residence record number and without renewing the software each year ».[365]

En Europe, un projet de règlement eIDAS2 est présentement sous étude, notamment parce que :

> « Il ressort de l'évaluation du règlement eIDAS que, dans sa version actuelle, cet instrument n'est pas en mesure de répondre à ces nouvelles demandes du marché, principalement pour les raisons suivantes : les limitations au secteur public qui lui sont inhérentes, les possibilités limitées et la difficulté pour les prestataires privés de services en ligne de se connecter au système, la disponibilité insuffisante de solutions d'identification électronique notifiées dans tous les États membres, et un manque de souplesse pour répondre à des cas d'utilisation variés. En outre, les solutions d'identité qui ne relèvent pas du champ d'application du règlement eIDAS, telles que celles proposées par les fournisseurs de médias sociaux et les établissements financiers, suscitent des inquiétudes quant au respect de la vie privée et à la protection des données. Elles ne peuvent pas satisfaire efficacement aux nouvelles demandes du marché et n'ont pas la portée transfrontalière nécessaire pour

---

361 *Règlement sur l'identification numérique*, YD 2022/164.

362 *Improving Digital Identity Act of 2023*, art. 2.

363 *Digital Signature Act*, art. 5(3) (Corée du Sud), en ligne : <https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=55068&type=part&key=43>.

364 « Digital Identification in Korea », (2021), en ligne : <https://dgovkorea.go.kr/contents/blog/111>.

365 « South Korea Plans to Launch Digital Identity Based on Blockchain Technology », (2023), en ligne : <https://ibtekr.org/en/cases/south-korea-plans-to-launch-digital-identity-based-on-blockchain-technology/>.

répondre à des besoins sectoriels pour lesquels l'identification est un aspect sensible et requiert un niveau élevé de certitude. »[366]

L'analyse se conclut en précisant que : « [l]es principales conclusions de l'évaluation en ce qui concerne l'identité électronique sont que le règlement eIDAS n'a pas atteint son potentiel »[367]. Ainsi, eIDAS2 propose :

> « [u]ne approche plus harmonisée au niveau de l'UE, fondée sur une transition fondamentale qui verrait l'abandon du recours aux seules solutions d'identité numérique au profit de la fourniture d'attestations électroniques d'attributs, permettrait aux citoyens et aux entreprises d'avoir accès à des services publics et privés partout dans l'UE s'appuyant sur des preuves d'identité et d'attributs vérifiés ».

2.3.1.4 Absence de tendance relative à certains nouveaux développements

2.3.1.4.1 Les chaînes de blocs

« Blockchain-based SSIs ». Tel que nous l'avons indiqué ci-dessus (2.3.1.2), l'une des tendances observées vise à adopter une approche plutôt agnostique quant aux types de technologies pouvant être utilisées pour procéder à l'identification/authentification des individus et, donc, de ne pas favoriser de technologies particulières. Toutefois, certains auteurs prônent une approche basée sur les « blockchain-based self-sovereign identities (SSIs) »[368]. Comme l'expliquent ceux-ci : « SSI enables citizens to control their data and share these with others. Hence, there is a shift from the government as a steward for their identity data to the citizens who control their own identity data »[369]. Cette proposition s'inscrit donc en opposition avec l'adoption d'une identité numérique régalienne. Si nous n'avons identifié aucune juridiction ayant opté d'encadrer cette approche, il importe de souligner que la Corée du Sud a tout au moins choisi de miser sur la technologie des chaînes de blocs. Ainsi, l'article 6 du *Digital Signature Act* prévoyait déjà que le gouvernement « shall endeavor to facilitate the use of various electronic-signature-creation devices, such as biometric authentication and blockchain »[370]. Or, il appert que cette possibilité a depuis été mise en œuvre :

> « The government abolished the exclusive use of accredited certificates in 2020 to promote convenient and reliable new electronic signature services by applying various new

---

366 *Proposition de Règlement du parlement européen et du conseil modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique*, exposé des motifs.

367 *Id*.

368 Voir Katharina KOERNER, « Self-Sovereign Identity as Future Privacy by Design Solution in Digital Identity ? », (2022) *IAPP*, en ligne :<https://iapp.org/media/pdf/resource_center/self-sovereign-identity-whitepaper.pdf>.

369 Rachel BENCHAYA GANS, Jolien UBACHT et Marijn JANSSEN, « Governance and Societal Impact of Blockchain-Based Self-Sovereign Identities », (2022) 41-3 *Policy and Society* 402, 403.

370 *Digital Signature Act*, art. 6(1) (Corée du Sud), en ligne : <https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=55068&type=part&key=43>.

technologies such as blockchains and biometrics in an effort to stimulate greater competitiveness in the electronic signature market. »[371]

Notons toutefois que cette décision a fait l'objet de critiques. En effet :

> « [l]'autorité de protection des données de Corée du Sud (PIPC) considère que l'un des sujets principaux concernant les services basés sur la blockchain est l'absence de possibilité de destruction des données. Les personnes ne peuvent plus faire valoir leur droit à l'oubli. Pour résoudre ces questions, la PIPC recommande ainsi aux services utilisant une blockchain de choisir une mise en œuvre qui ne stocke pas de données sur la chaîne de blocs elle-même (les données peuvent être stockées hors chaîne ou sur une chaîne latérale). »[372]

Étant d'avis que la chaîne de blocs se présente comme solution en quête de problème là où les intermédiaires de confiance sont absents, l'approche coréenne nous semble toutefois peu adaptée au modèle québécois. Sans rejeter son utilisation, il nous appert peu utile de reproduire l'erreur des législateurs ayant choisi d'encadrer l'usage des signatures numériques et de maintenir l'approche technologiquement neutre qui a – jusqu'à présent – bien servi l'État et les citoyens québécois.

2.3.1.4.2 L'hypertrucage

Absence de cadre propre. Bien que la question de l'hypertrucage soit abordée ailleurs dans la présente étude[373], il importe de souligner que cette problématique aura également une incidence sur l'identité puisque des cas d'hypertrucages vocaux[374] et visuels[375] ont déjà mené à de fausses confirmations d'identité. Toutefois, nous n'avons répertorié aucun cas de document législatif propre à l'hypertrucage lié à la question de l'identité. En fait, selon nos recherches, seule la Chine a procédé à l'adoption d'un cadre réglementaire propre à ces questions[376] et celui-ci ne touche pas aux questions d'identité[377]. Évidemment, comme une image hypertruquée constitue un faux au sens

---

371 « Digital Identification in Korea », (2021), en ligne : <https://dgovkorea.go.kr/contents/blog/111>.

372 COMMISSION NATIONALE INFORMATIQUE ET DES LIBERTÉS, « L'identité numérique », (2023), en ligne : <https://www.cnil.fr/sites/cnil/files/2023-03/CNIL_Dossier-thematique_Identite%20numerique.pdf>, p. 12.

373 *Supra*, Section 2.2.1.3.

374 L'IA utilisée pour recréer la voix d'un PDG et voler 320 000 $ à une entreprise. *Radio Canad*a, (2019, 4 septembre), en ligne : <https://ici.radio-canada.ca/nouvelle/1287053/deepfaker-hypertrucage-fraude-pdg-euler-hermes-group>.

375 Voir par exemple, P. SAINT-ARNAUD, « Premiers contacts avec l'hypertrucage sous les traits de Bernard Derome », *La Presse,* (2020, février), en ligne : <https://www.lapresse.ca/affaires/techno/2020-02-09/premiers-contacts-avec-l-hypertrucage-sous-les-traits-de-bernard-derome>.

376 Tiffany HSU, « As Deepfakes Flourish, Countries Struggle with Response », (2023) *New York Times*, en ligne : <https://www.nytimes.com/2023/01/22/business/media/deepfake-regulation-difficulty.html>.

377 CHINA NETWORK INFORMATION NETWORK, « The Cyberspace Administration of China and Other Three Departments Issued the Regulations on the In-depth Synthesis Management of Internet Information Services », (2022) en ligne : <http://www.cac.gov.cn/2022-12/11/c_1672221949318230.htm>.

de l'article 258 du *Code de procédure civile*[378], l'adoption de dispositions propres à l'hypertrucage en matière d'identité ne semble pas indiquée.

PROPOSITION #17 : Retirer les dispositions relatives aux données biométriques de la LCCJTI et les transposer vers la *Loi sur la protection des renseignements personnels dans le secteur privé*[379] ainsi que la *Loi sur l'accès aux documents des organismes publics et la protection des renseignements personnels*[380], d'une part, afin de regrouper au sein des mêmes documents législatifs les dispositions devant être appliquées par la Commission d'accès à l'information et, d'autre part, par souci de cohérence propre aux objets visés, à savoir des données biométriques lesquelles constituent des renseignements personnels.

PROPOSITION #18 : Réviser les articles 40 à 62 LCCJTI afin de s'assurer que ceux-ci ne reflètent pas seulement les infrastructures à clé publique pour plutôt mettre de l'avant une approche associée aux identités numériques. À cette fin la norme *Digital Trust and Identity*[381] pourrait servir d'inspiration.

PROPOSITION #19 : La migration vers un système d'identités numériques renferme divers risques propres à la surveillance et au profilage des citoyens[382]. L'approche devrait donc faire l'objet d'analyses d'incidences afin d'éviter d'importantes conséquences négatives pour la vie privée des citoyens[383].

2.4 LCCJTI + sécurité

Mise en contexte. Lors de son adoption en 2001, la LCCJTI faisait en quelque sorte école à part en adoptant une vision de la sécurité de l'information fondée sur la « triade DIC » qui dépassait celle des renseignements personnels. En effet, rappelons que l'obligation de sécurité s'articule autour de trois principaux piliers, à savoir : la disponibilité, l'intégrité et la confidentialité des données.

La disponibilité, soit la « propriété d'être accessible et utilisable à la demande par une entité autorisée »[384] est souvent l'enfant pauvre en matière de sécurité puisque l'accent qui est mis sur l'obligation d'assurer la confidentialité de certaines données viendra nécessairement nuire à la

---

378 RLRQ c C-25.01.

379 RLRQ c P-39.1.

380 RLRQ c A-2.1.

381 CAN/CIOSC 103-1:2020 *Digital Trust and Identity – Part 1 : Fundamentals*, en ligne : <https://www.scc.ca/fr/standardsdb/standards/30660>.

382 COMMISSION NATIONALE INFORMATIQUE ET DES LIBERTÉS, « L'identité numérique », (2023), en ligne : <https://www.cnil.fr/sites/cnil/files/2023-03/CNIL_Dossier-thematique_Identite%20numerique.pdf>, p. 2.

383 « Opinion of the European Economic and Social Committee on Digital Identity, Data Sovereignty and the Path to a Just Digital Transition for Citizens Living in the Information Society (Own-Initiative Opinion) », 2022/C 443/03, par. 1.7.

384 Norme ISO/IEC 27000:2018(fr) – Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire, par. 3.7.

disponibilité de celles-ci. En effet, comme le soulignent John Viega et Gary McGraw[385] : « [t]he most secure computer in the world is one that has its disk wiped, is turned off, and is buried in a 10-foot hole filled with concrete. Of course, a machine that secure also turns out to be useless ». L'obligation d'assurer la disponibilité des données – et nous ajouterions une certaine sous-obligation de convivialité puisqu'une information disponible aux seules personnes bénéficiant d'une expertise poussée en informatique n'est pas réellement disponible – s'avère donc être en constante compétition avec l'obligation de confidentialité[386]. En effet, « the easier it is to access something, the less secure it is likely to be »[387]. Il importe donc d'assurer un équilibre entre ces deux obligations puisque, malgré l'accent mis sur la confidentialité par les législateurs (nous y reviendrons), les données se doivent d'être « accessibles dans les délais convenables pour les personnes autorisées à en disposer dès qu'elles le désirent »[388], d'abord pour des raisons juridiques[389] ensuite parce qu'une information qui n'est pas disponible pour les parties à une séance de négociation ou de médiation s'avère inutile.

Quant à elle, l'intégrité se résume à la « propriété d'exactitude et de complétude » de l'information[390], ou, pour être plus explicite, à « [l]a propriété d'être conservé intact, sans dommage et sans perte, et de n'être détruit ou transformé que par l'intervention des personnes autorisées à le faire »[391]. Législativement, ce même concept est défini à l'article 6 LCCJTI de la façon suivante : « [l]'intégrité du document est assurée, lorsqu'il est possible de vérifier que l'information n'en est pas altérée et qu'elle est maintenue dans son intégralité, et que le support qui porte cette information lui procure la stabilité et la pérennité voulue »[392]. En effet, une donnée dont l'intégrité est compromise devient souvent inutile. L'article 6 LCCJTI poursuit en précisant que : « [l]'intégrité du document doit être maintenue au cours de son cycle de vie, soit depuis sa création, en passant par son transfert, sa consultation et sa transmission, jusqu'à sa conservation, y compris son archivage ou sa destruction », alors que l'article 19 du même texte de loi vient ajouter que « [t]oute personne doit, pendant la période où elle est tenue de conserver un document, assurer le maintien

---

385 Tels que cités par David LAROCHELLE et Nicholas ROSASCO, « Towards a Model of the Costs of Security », (2003), en ligne : <https://docplayer.net/210454401-Towards-a-model-of-the-costs-of-security.html>, p. 2.

386 Dave TYSON, *Security Convergence : Managing Enterprise Security Risk*, Burlington, Butterworth-Heinemann, 2007, p. 70, « ease of use creates security weaknesses, whereas a stronger security posture generally reduces functionality of user overhead and administration ».

387 Dave TYSON, *Security Convergence: Managing Enterprise Security Risk*, Burlington, Butterworth-Heinemann, 2007, p. 70.

388 Joël HUBIN et Yves POULLET, *La sécurité informatique, entre technique et droit*, Namur, C.R.I.D., 1998, p. 7.

389 Voir notamment René VERGÉ, « Dimensions légales et éthiques des technologies de l'information », dans Abdelhaq ELBEKKALI, *Gouvernance, audit et sécurité des TI*, Brossard, CCH, 2008, p. 89, à la page 134 : « une organisation a été négligente si, suite à un incendie, elle n'était pas en mesure de récupérer les données essentielles à la poursuite de ses affaires. Même si une simple copie de sauvegarde des données aurait pu prévenir ce genre de problème, l'organisation pourrait dans cette situation faire face à des poursuites de la part de ses clients, de ses employés, de ses actionnaires et de plusieurs autres parties affectées ».

390 Norme ISO/IEC 27000:2018(fr) – Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire, par. 3.36.

391 Joël HUBIN et Yves POULLET, *La sécurité informatique, entre technique et droit*, Namur, C.R.I.D., 1998, p. 7.

392 Loi *concernant le cadre juridique des technologies de l'information*, RLRQ c C-1.1, art. 6.

de son intégrité et voir à la disponibilité du matériel qui permet de le rendre accessible et intelligible et de l'utiliser aux fins auxquelles il est destiné ».

Finalement, la confidentialité, soit la « propriété selon laquelle l'information n'est pas diffusée ni divulguée à des personnes, des entités ou des processus non autorisés »[393] demeure l'élément le plus couramment associé à la notion de sécurité. Au Québec, cette obligation est principalement énoncée à l'article 25 LCCJTI, laquelle disposition prévoit que :

> « La personne responsable de l'accès à un document technologique qui porte un renseignement confidentiel doit prendre les mesures de sécurité propres à en assurer la confidentialité, notamment par un contrôle d'accès effectué au moyen d'un procédé de visibilité réduite ou d'un procédé qui empêche une personne non autorisée de prendre connaissance du renseignement ou, selon le cas, d'avoir accès autrement au document ou aux composantes qui permettent d'y accéder. »

Comme nous le verrons, la référence à ce triptyque au sein de différents efforts législatifs à travers le monde a explosé au fil des 20 dernières années. Toutefois, l'approche québécoise d'aborder le renseignement confidentiel plutôt que le seul renseignement personnel demeure peu répandu.

2.4.1 État des tendances

Tendance générale. Avant d'aborder les diverses tendances observées et évaluées, il importe de souligner une tendance générale en matière de sécurité, soit celle d'une relative inflation législative propre aux politiques, dispositions et textes de loi relatifs à la sécurité de l'information et à la cybersécurité[394]. Par exemple, aux États-Unis, une étude rapporte l'adoption de 500 textes législatifs et autant de politiques portant sur ces questions[395]. Plusieurs de ces textes viennent de la cybersécurité en matière pénale ou la sécurité des infrastructures publiques – des thématiques externes à l'application de la LCCJTI – mais le constat d'une attention grandissante à la sécurité par les législateurs demeure valide.

Ceci crée évidemment un contraste évident avec l'état du droit au niveau international relatif à la sécurité de l'information lors de l'adoption de la *Loi concernant le cadre juridique des technologies de l'information*. Rappelons que, à cette époque, même la famille de norme ISO relatives à la

---

393 Norme ISO/IEC 27000:2018(fr) – Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire, par. 3.10.

394 Nous limitons ici la cybersécurité à la « [c]apacité, pour un système en réseau, de se protéger et de résister à des événements issus du cyberespace et susceptibles de porter atteinte à la confidentialité, à l'intégrité et à la disponibilité de l'information qu'il contient », voir en ligne : <https://www.quebec.ca/gouvernement/politiques-orientations/vitrine-numeriqc/politique-gouvernementale-de-cybersecurite/definitions>. Alors que la sécurité de l'information vise l'« [e]nsemble de mesures mises en place pour assurer la protection des informations selon le niveau de confidentialité, d'intégrité et de disponibilité jugé nécessaire », voir en ligne : <https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/8358572/securite-de-linformation>. Cette approche nous permet ainsi de faire la distinction entre la protection du contenu « les informations » et le contenant « un système en réseau ».

395 Adam ALEXANDER, Paul GRAHAM, Eric JACKSON, Bryant JOHNSON, Tania WILLIAMS, Jaehong PARK, « An Analysis of Cybersecurity Legislation and Policy Creation on the State Level », (2019) *NCS*, p. 35, en ligne : < https://link.springer.com/content/pdf/10.1007/978-3-030-31239-8_3.pdf >.

sécurité (27000) n'avait pas encore été créée. En fait, la norme BS7799 sur laquelle la norme ISO est basée n'a elle-même été créée qu'en 1995, puis adoptée par l'ISO sous la cote ISO/IEC 17799 en 2000, c'est-à-dire quelques mois avant l'adoption de la LCCJTI. Ainsi, bien que la triade DIC présentée ci-dessus soit aujourd'hui acceptée presque universellement comme constituant les fondements de la sécurité de l'information[396], ce constat demeure relativement récent.

Plan. S'il est indéniable que la disponibilité, l'intégrité et la confidentialité des renseignements – principalement des renseignements personnels – constituent aujourd'hui une préoccupation importante pour les législateurs d'ici (*Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*) et d'ailleurs (RGPD), on constate un fractionnement et une multiplication des dispositions relatives à la cybersécurité selon diverses approches proposant une analyse en silo (2.4.1.1), à savoir : une approche sectorielle (droit de la consommation, droit du travail, droit bancaire, etc.)), fonctionnelle (anonymisation, profilage, etc.), ou technologique (intelligence artificielle, chaîne de blocs, etc.). Pour les raisons invoquées ci-dessous, cette tendance nous semble problématique et risquée au niveau temporel puisqu'elle pourrait mal évoluer. Une tendance nous semblant avoir plus de mérite voit une plus grande pénétration de l'analyse de risques dans les textes législatifs (2.4.1.2), ce qui correspond à une approche favorisée par la doctrine depuis déjà quelques années. Finalement, tel que nous l'avons soulevé à plusieurs endroits dans le présent rapport, nous constatons une déférence grandissante à l'égard de normes techniques (principalement la norme ISO 27001) (2.4.1.3) qui mérite que l'on s'y attarde.

2.4.1.1 Tendance vers une analyse en silo des thématiques de sécurité

2.4.1.1.1 Tendance vers une approche sectorielle des thématiques de sécurité

Une première tendance que l'on peut observer au niveau international est celle d'aborder la sécurité par thématique, c'est-à-dire d'y référer dans divers textes législatifs propres à un type de donnée (contenu)[397] ou d'infrastructure (contenant) plutôt que d'adopter une approche holistique similaire à celle proposée par la LCCJTI.

Les législateurs américains constituent l'exemple le plus extrême de cette approche puisque, ne possédant aucune loi transversale sur la protection des renseignements personnels et encore moins sur la protection des données en général, ils ont adopté au fil des ans une panoplie de lois thématiques possédant certaines dispositions propres à la sécurité de l'information[398]. La tendance est ainsi on ne peut plus claire et est d'ailleurs annoncée. En effet, la *National Cybersecurity*

---

396 J. FRUHLINGER, « The CIA Triad : Definition, Components and Examples, *CSO Online*, (2020, 10 février), en ligne : <https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html>.

397 Pensons par exemple aux données ouvertes. Voir : *Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (refonte)*, PE/28/2019/REV/1.

398 ACRONIS, *Data Sovereignty Around the World : Exploring Regulations in Canada, U.S., U.K., E.U., Brazil and Japan*, en ligne : <https://dl.acronis.com/u/rc/White-Paper-Acronis-Cyber-Protect-Cloud-Data-Sovereignty-Around-the-World-EN-US.pdf>.

Strategy[399] étatsunienne prévoit que « The Federal Government will use existing authorities to set necessary cybersecurity requirements in critical sectors »[400]. On voit naître divers projets régulatoires visant la sécurité des renseignements personnels émerger de la Federal Trade Commission (FTC) et du Securities and Exchange Commission (SEC) dans leurs secteurs de compétences respectifs[401]. Aussi, plutôt que d'adopter des lois visant la sécurité de l'information en général, plusieurs États étudient l'adoption de lois sur la protection des renseignements personnels des consommateurs[402] (approche notamment déjà privilégiée en Californie[403] et également proposée par le gouvernement canadien[404]).

Au Canada, cette approche sectorielle s'observe notamment par une volonté d'adopter des règles sécuritaires propres au secteur financier[405] et, comme nous venons de le souligner, la protection des renseignements personnels des consommateurs[406].

Notons par ailleurs qu'une approche de la sécurité se concentrant uniquement sur la protection des renseignements personnels est en soi « thématique » et nous appert de ce fait problématique. Pour illustrer notre propos, prenons l'article 32 du *Règlement général sur la protection des données*, lequel impose l'obligation suivant :

> « Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins […] des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement. »

---

399 THE WHITE HOUSE, *National Cybersecurity Strategy*, (2023, mars), en ligne : <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>.

400 THE WHITE HOUSE, *National Cybersecurity Strategy*, (2023, mars), en ligne : <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>, p. 8.

401 Poona BHASKAR, Christopher M. Caparelli, « FTC Headline a Rise in U.S. Privacy And Cybersecurity Efforts SEC », (2023), *Lexology*, en ligne: <https://www.lexology.com/library/detail.aspx?g=c165047b-d3cf-4d2b-8203-848f444432ae&utm_source=Lexology+Daily+Newsfeed&utm_medium=HTML+email+-+Body+-+General+section&utm_campaign=ITCan+subscriber+daily+feed&utm_content=Lexology+Daily+Newsfeed+2023-07-27&utm_term=>.

402 *Id.*

403 *California Consumer Privacy Act of 2018*.

404 Projet de loi C-27 : *Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois*, juin 2022.

405 COMITÉ PERMANENT DE LA SÉCURITÉ PUBLIQUE ET NATIONALE, C*ybersécurité dans le secteur financier comme un enjeu de sécurité nationale*, (2019, juin), en ligne : <https://www.ourcommons.ca/DocumentViewer/fr/42-1/SECU/rapport-38/>.

406 Projet de loi C-27 : *Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois*, juin 2022.

Si cette disposition nous appert relativement complète et s'inscrit dans la tendance observée tant au niveau des initiatives étatiques[407], que normatives[408], elle ne s'applique qu'aux « données à caractère personnel »[409]. Ainsi, les autres types de données confidentielles, notamment les secrets commerciaux, ne bénéficient pas d'une protection identique. Soit, la Directive 2022/2555[410] vient corriger cette approche en créant une obligation de « résister, à un niveau de confiance donné, à tout événement susceptible de compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement »[411], mais cette obligation vient s'appliquer aux seuls fournisseurs de service numérique et non à ceux qui contrôlent lesdites données[412].

La Chine, de son côté, semble privilégier une approche holistique[413]. En effet, la *Data Security Law* ne s'intéresse pas à un type particulier de données, mais sépare l'ensemble des données en deux catégories devant bénéficier d'un niveau de sécurité distinct :

- **Core data** : « any data that concerns Chinese national and economic security, Chinese citizens' welfare and significant public interests »[414];
- **Important data** : « the next-most sensitive level of data »[415].

---

407 *Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2)* (Texte présentant de l'intérêt pour l'EEE), PE/32/2022/REV/2.

408 Par exemple, voir le Department for Digital, Culture, Media & Sport. The NIS Regulation 2018, (avril 2018), en ligne : <https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018#:~:text=The%20Security%20of%20Network%20%26%20Information,essential%20services%20and%20digital%20services/>.

409 L'article 4 du RGPD définit les données à caractère personnel comme suit : « toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée"); est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».

410 *Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2)* (Texte présentant de l'intérêt pour l'EEE), PE/32/2022/REV/2.

411 Article 6 de la Directive.

412 Sur la notion de contrôle, voir le livre de Vincent GAUTRAIS et Pierre TRUDEL, C*irculation des renseignements personnels et Web 2.0*, Montréal, Éditions Thémis, 2010.

413 Notons ici que, pour des raisons linguistiques, nous travaillons évidemment à partir de sources secondaires et ne pouvons confirmer l'exactitude des contenus cités.

414 D. JUNCK, R. A. KLEIN, B. KUMAKI, A. D. KUMAYAMA, K. KWOK, S. D. LEVI, S. TALBOT, J. VERMYUNCK, E. ZHANG, S., « China's New Data Security and Personal Information Protection Laws : What They Mean for Multinational Companies, *Skadden, Arps, Slate, Meagher & Flom LLP*, (2021, 3 novembre), en ligne : <https://www.skadden.com/insights/publications/2021/11/chinas-new-data-security-and-personal-information-protection-laws>.

415 *Id.*

Selon les sources consultées, le « core data » doit bénéficier d'un niveau élevé de protection et donc d'un cadre législatif qui reflète ce niveau, alors que les autorités chinoises doivent publier incessamment une liste des types de données pouvant être qualifiées d'« importantes »[416]. Il nous faudra attendre pour voir quelles données peuvent être qualifiées d'importantes, mais cette approche n'est pas sans rappeler la catégorisation des renseignements personnels selon leur niveau de sensibilité prévu notamment à l'article 3.7 de la *Loi sur la protection des renseignements personnels dans le secteur privé*, obligation créée à la suite de l'adoption de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*[417].

Finalement, bien qu'elle soit extérieure à l'objet de la *Loi concernant le cadre juridique des technologies de l'information* et se compare plutôt à l'adoption de la *Loi édictant la Loi sur le ministère de la Cybersécurité et du Numérique et modifiant d'autres dispositions*[418], une tendance identifiée dans bon nombre de juridictions vise l'adoption de règles propres aux infrastructures technologiques et systèmes d'information[419] (c'est notamment le cas du projet de loi C-26 au Canada[420]), particulièrement en matière de sécurité nationale[421], ou pour favoriser le commerce[422].

2.4.1.1.2 Tendance vers une approche fonctionnelle des thématiques de sécurité

Cette tendance s'observe à deux niveaux. Au niveau macro, on constate une multiplication de textes visant une thématique fonctionnelle particulière. Par exemple, aux États-Unis, « [e]very state has enacted laws directed at protecting state governments and businesses specifically from cyberintrusions »[423]. Ce n'est donc pas l'objet (par ex. : le renseignement confidentiel) qui est visé, mais le type de menace à sa sécurité.

---

416 *Id.*

417 LQ 2021, c 25.

418 LQ 2021, c 33.

419 Department for Digital, Culture, Media & Sport, *The NIS Regulation 2018*, (2018, avril), en ligne : <https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018#:~:text=The%20Security%20of%20Network%20%26%20Information,essential%20services%20and%20digital%20services/>.

420 *Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois*, Projet de loi nº C-26 (1re lecture – 14 juin 2022) 1re session, 44e législature (Can).

421 *Cybersecurity Act* of 2015. Voir également en ligne : <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>.

422 Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (Texte présentant de l'intérêt pour l'EEE), PE/32/2022/REV/2; Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) nº 526/2013 (règlement sur la cybersécurité) (Texte présentant de l'intérêt pour l'EEE), PE/86/2018/REV/1.

423 M. J. Glennon, *State-level Cybersecurity*, Policy Rev. 171, 85–102 (2012), en ligne : <https://link.springer.com/content/pdf/10.1007/978-3-030-31239-8_3.pdf>.

Au niveau micro, on constate l'adoption de normes ou de dispositions propres à une technologie ou un mécanisme à mettre en place (par ex. : l'anonymisation des données[424]). Tel que nous l'avons vu dans la section précédente relative à l'identité (2.3), cette approche est risquée puisqu'elle présume que certains mécanismes et certaines technologies n'ayant pas nécessairement fait leur preuve demeureront pertinents dans les années à venir.

2.4.1.1.3 Tendance vers une approche technologique des thématiques de sécurité

Une dernière tendance s'inscrivant dans cette analyse en silo que nous critiquons – celle-ci beaucoup plus évidente – concerne une approche visant à aborder la sécurité selon la technologie ou les technologies utilisées. C'est ainsi que la Maison Blanche propose des directives de sécurité propres à l'Internet des objets[425], ou que l'on constate l'émergence de dispositions sécuritaires propres aux environnements d'infonuagique[426] ou de l'Internet[427].

L'exemple le plus fragrant de cette tendance est certainement celui de l'intelligence artificielle. En effet, « work is increasingly being dedicated to the topic [of AI-spectific security] in form of reports, studies and first international standardisation work items »[428]. Ainsi, dans le même ordre d'idées, l'article 10 du projet de *Législation sur l'intelligence artificielle* européen [429] prévoit que « l'utilisation des mesures les plus avancées en matière de sécurité et de protection de la vie privée, telles que la pseudonymisation, ou le cryptage lorsque l'anonymisation peut avoir une incidence significative sur l'objectif poursuivi », alors que l'article 15 du même projet de règlement vise notamment l'adoption de « solutions techniques visant à garantir la cybersécurité des systèmes d'IA à haut risque ».

Notons que le projet de règlement européen propose toutefois une approche qui s'éloigne parfois du silo que l'on observe dans d'autres juridictions puisqu'il n'offre pas un niveau de détail important quant aux exigences de sécurité préférant faire des renvois à d'autres documents

---

424 RGPD.

425 Townsend L. BOURNE, Lillia DAMALOUJI, « Cybersecurity Labeling Program to Increase Transparency of IoT Device Security », (2023), *Lexology,* en ligne : <https://www.lexology.com/library/detail.aspx?g=3e9e6ae7-567d-4192-83dd-0c89388ffd9d&utm_source=Lexology+Daily+Newsfeed&utm_medium=HTML+email+-+Body++General+section&utm_campaign=ITCan+subscriber+daily+feed&utm_content=Lexology+Daily+Newsfeed+2023-08-07&utm_term=>.

426 FUTURE INTERNATIONAL CENTRE FOR CRIMINAL LAW REFORM & CRIMINAL JUSTICE POLICY, Canada's Future CLOUD Act Agreement with the United States, (2022, 29 mars), en ligne : <https://icclr.org/2022/03/29/canadas-future-cloud-act-agreement-with-the-united-states/>.

427 THE WHITE HOUSE, *National Cybersecurity Strategy*, (2023, mars), <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>, p. 30.

428 Henrik JUNKLEWITZ *et al*, « Cybersecurity of Artificial Intelligence in the AI Act, (2023) *UE*, en ligne : <https://op.europa.eu/fr/publication-detail/-/publication/7d0a4007-51dd-11ee-9220-01aa75ed71a1/language-en>, p. 5.

429 Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union, COM/2021/206 final.

normatifs tels le Règlement (UE) 2019/881 du Parlement européen et du Conseil[430](art. 42) concernant l'obligation d'obtenir une forme de certification. Cette approche nous semble préférable puisqu'elle évite les risques de doublons, de redondances et, surtout, d'incohérence entre textes de loi.

Finalement, mentionnons que cette approche sectorielle n'est pas propre aux législateurs. Elle est aussi présente dans l'univers normatif. Ainsi, ISO a développé des normes propres à la sécurité des environnements d'infonuagique[431] et œuvre présentement au développement d'une norme propre à la cybersécurité et l'IA[432]. Sans nous prononcer sur la norme ISO 27090, puisque celle-ci n'est pas encore disponible, la norme ISO 27018 n'apporte guère de nouveaux éléments à la norme ISO 27001. Ainsi, comme en matière législative, l'on peut se questionner sur la pertinence d'une telle approche technologique. Par cynisme, l'on pourrait prétendre que celle-ci se justifie par une nécessité de générer de nouveaux revenus, mais nous soumettons que la problématique est plus large. Elle découle souvent d'une méconnaissance des technologies visées et de leur possible évolution, et donc d'un désir de prévoir l'imprévisible.

2.4.1.2 Tendance vers une plus grande pénétration de l'analyse de risques dans les textes législatifs

Si nous demeurons sceptiques quant aux bienfaits des approches en silo analysées ci-dessus, une autre tendance qui nous semble plus utile est celle de valoriser l'analyse de risques comme composante de l'obligation de sécurité. En effet, rappelons que les dictionnaires juridiques définissent la sécurité comme étant l'état de celui qui est à l'abri des risques[433]. Ainsi, pour augmenter la sécurité, il importe de contrôler – dans les limites de ce qui est possible – les risques auxquels nous sommes soumis, nécessitant de ce fait d'effectuer une analyse de risques. Notons que cette thèse a d'abord été développée en droit québécois par l'un des auteurs du présent rapport[434]. Elle semble toutefois aujourd'hui avoir reçu l'aval de divers législateurs[435], notamment des rédacteurs de l'Accord Canada-États-Unis-Mexique (ACEUM). En effet, l'article 19.15 de l'ACEUM prévoit que :

> « Étant donné le caractère évolutif des menaces contre la cybersécurité, les Parties reconnaissent que des approches fondées sur le risque pourraient être plus efficaces qu'une réglementation normative pour faire face à ces menaces. Par conséquent, chacune des

---

430 Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013 (règlement sur la cybersécurité) (Texte présentant de l'intérêt pour l'EEE), PE/86/2018/REV/1.

431 ISO/IEC 27018:2019 - Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII.

432 Norme ISO 27090. Voir : <https://www.iso.org/standard/56581.htm>l.

433 Gérard CORNU, V*ocabulaire juridique,* Paris, PUF, 2007, p. 853; et Hubert REID.

434 Nicolas W. VERMEYS, *Responsabilité civile et sécurité informationnelle*, Cowansville, Éditions Yvon Blais, 2010.

435 Par exemple, dans son exposé des motifs, le projet européen de Législation sur l'intelligence artificielle propose « une approche proportionnée fondée sur le risque ».

> Parties s'efforce d'adopter, et encourage les entreprises qui relèvent de sa juridiction à adopter, des approches fondées sur le risque qui s'appuient sur des normes consensuelles et des pratiques exemplaires de gestion du risque pour détecter les risques liés à la cybersécurité et assurer une protection contre ces derniers, ainsi que pour détecter les événements liés à la cybersécurité, y réagir et y remédier. » (Notre soulignement)

Comme le Québec est visé par certaines dispositions de l'ACEUM – soit celles qui sont liées à ses champs de compétence – l'adoption d'une telle approche pourrait être envisagée, d'autant qu'elle semble déjà avoir été prise en compte lors de la réforme relative aux lois en matière de protection des renseignements personnels[436], sujet connexe à l'objet de la présente section de l'étude. En effet, pour ne prendre que cet exemple, les nouveaux articles 63.8 et 63.10 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[437] imposent indirectement une analyse de risques de sécurité.

2.4.1.3 Tendance vers une délégation de pouvoir aux organismes normatifs

Une autre tendance importante en matière d'encadrement des obligations relatives à la sécurité des données réside dans une délégation du pouvoir législatif vers des organismes normatifs[438] (voir la section 2.1.1). Pour ne citer que cet exemple, le considérant 61 du projet de *Législation sur l'intelligence artificielle* prévoit que :

> « La normalisation devrait jouer un rôle essentiel pour fournir des solutions techniques aux fournisseurs afin de garantir la conformité avec présent règlement. Le respect des normes harmonisées telles que définies dans le règlement (UE) nº 1025/2012 du Parlement européen et du Conseil devrait être un moyen pour les fournisseurs de démontrer la conformité aux exigences du présent règlement. Cependant, la Commission pourrait adopter des spécifications techniques communes dans les domaines où il n'existe pas de normes harmonisées ou où elles sont insuffisantes. »[439]

L'article 25 de la Directive (UE) 2022/2555 est au même effet :

> « Afin de favoriser la mise en œuvre convergente de l'article 21, paragraphes 1 et 2, les États membres encouragent, sans imposer l'utilisation d'un type particulier de technologies ni créer de discrimination en faveur d'un tel type particulier de technologies, le recours à des normes et des spécifications techniques européennes et internationales pour la sécurité des réseaux et des systèmes d'information. »

---

436 *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, LQ 2021, c 25.

437 RLRQ c A-2.1.

438 Voir par exemple l'article 501 du *Cybersecurity Enhansement Act* of 2014, laquelle disposition vise le développement de standards internationaux de sécurité et collaboration avec le secteur privé.

439 Pour une analyse de cette disposition, voir Henrik JUNKLEWITZ *et al*, « Cybersecurity of artificial intelligence in the AI Act », (2023) *UE*, en ligne : <https://op.europa.eu/fr/publication-detail/-/publication/7d0a4007-51dd-11ee-9220-01aa75ed71a1/language-en>, p. 7.

Si cette approche s'explique notamment par une nécessaire flexibilité dans l'élaboration de règles propres à la sécurité en général et à la cybersécurité en particulier, elle soulève diverses questions relatives à la légitimité de cette forme de « droit mou » (*soft law*) et à son effectivité : les normes étant nombreuses, souvent floues, dispendieuses et développées en fonction des intérêts d'acteurs particuliers[440].

PROPOSITION #20 : Tel qu'il découle de ce qui précède, notre première proposition est simple : nous sommes d'avis qu'il n'est pas opportun de suivre les tendances identifiées. En effet, tel que nous l'avons soulevé, ces tendances nous semblent aller dans la mauvaise direction, c'est-à-dire, d'une part, de générer un corpus législatif « hyperspécialisé » qui risque d'échapper – tel qu'on le voit déjà notamment en matière de poursuites pour bris de sécurité – certains risques présents ou à venir. D'autre part, une trop grande déférence au droit mou que sont les normes soulève diverses questions. Soit il importe de tenir compte de ces normes, mais il faudrait éviter de leur donner une place prédominante et, de ce fait, abandonner à des organismes privés une partie des compétences du gouvernement du Québec. Le Comité d'harmonisation (voir section 1.2) pourrait – tel qu'il devait le faire à l'origine – contribuer à la réflexion sur ce point.

PROPOSITION #21 : Nous sommes d'avis que la rédaction des articles 25 et 26 LCCJTI mériterait une réécriture afin, d'une part, de clarifier leur portée et, d'autre part, de mieux présenter la triade disponibilité, intégrité, confidentialité et d'assurer une mise en valeur équivalente à ces trois concepts. En effet, l'article 25 s'intéresse présentement uniquement à la confidentialité, alors que l'article 26 prévoit l'obligation d'assurer la sécurité et d'en préserver l'intégrité et la confidentialité, ce qui s'avère redondant, la confidentialité et l'intégrité étant des composantes de la sécurité. Finalement, la disponibilité n'est pas citée à l'article 26. Elle n'est présente que si l'on interprète l'obligation d'« interdire l'accès [à un renseignement] à toute personne qui n'est pas habilitée à en prendre connaissance », *a contrario*, c'est-à-dire en présumant une obligation corolaire de permettre l'accès à ceux et celles qui sont habilités à en prendre connaissance. D'ailleurs, cette interprétation nous semble être la seule valable puisque, si l'on présume que le législateur ne parle pas pour rien dire[441], et comme interdire l'accès aux personnes non habilitées correspond à assurer la confidentialité d'une information – obligation déjà énumérée – alors on ne peut l'interpréter autrement. Cela étant, plutôt que de laisser aux tribunaux le rôle de trancher sur cette question, il nous appert pertinent de simplement clarifier le texte de ces dispositions.

Une approche plus robuste et détaillée viendrait par ailleurs créer un système de balises auquel le législateur pourra référer dans le cadre d'autres efforts législatifs afin d'éviter les doublons (pensons ici par exemple à l'art. 6 LCCJTI et l'art. 2839 C.c.Q. en matière d'intégrité) et de s'assurer qu'il n'y a pas de contradictions entre les différents textes qui réfèrent à ces notions.

---

440 Vincent GAUTRAIS, *Étude juridique sur la Loi concernant le cadre juridique des technologies de l'information* (RLRQ c C-1.1) – Mandat du ministère de la Justice du Québec, 31 juillet 2020. Voir également Nicolas W. VERMEYS, *Responsabilité civile et sécurité informationnelle*, Cowansville, Éditions Yvon Blais, 2010, p. 128 et ss.

441 *Théberge* c. *Galerie d'Art du Petit Champlain inc.*, [2002] 2 RCS 336, par. 142.

CONCLUSION

Pour conclure la présente étude, nous nous limiterons à réitérer les propositions formulées tout au long du rapport. Ainsi, nos recherches nous auront permis de constater que les éléments suivants devraient faire l'objet de réflexions de la part des ministères impliqués :

- **PROPOSITION #1 :** Si la notion de « technologie » semble particulièrement adaptée 20 ans plus tard, le spectre des opérations susceptibles d'être envisagées est en revanche désormais trop étroit. On pourrait donc envisager l'hypothèse de « **traitement** » comme nouvelle situation demandant un régime d'encadrement.

- **PROPOSITION #2 :** L'équivalence fonctionnelle est une notion clé largement utilisée dont la pertinence demeure. Il importe néanmoins d'analyser, selon la technologie que l'on cherche à encadrer, si le comparatif avec le support analogique est justifié.

- **PROPOSITION #3 :** La notion de neutralité technologique correspond à un principe rédactionnel somme toute assez classique et généralement reconnu. Son application est à favoriser sous réserve de spécificités liées à un secteur d'activité ou à la technologie elle-même. Si tel est le cas, un traitement spécifique doit être justifié.

- **PROPOSITION #4 :** Le choix d'une approche technologiquement spécifique doit, d'une part, être justifié et, d'autre part, être basé sur une définition précise qui permet aisément de déterminer le champ d'application.

- **PROPOSITION #5 :** Même si sa structuration n'a pas besoin de se comparer aux exemples européens, nous croyons que l'avènement de débats sociétaux importants en lien avec certaines évolutions technologiques pourrait être l'occasion de revigorer le rôle du Comité d'harmonisation, et ce, en conformité avec quelques amendements législatifs récents (2021) qui semblent offrir une plus grande liberté d'action audit comité.
  Le rôle du comité devrait être revu, au-delà de la seule harmonisation initialement prévue et s'étendre à un rôle plus large d'animation normative. Son rôle devra aussi être envisagé de concert avec celui qui prévaut dans la *Loi sur le ministère de la Cybersécurité et du Numérique*.

- **PROPOSITION #6 :** En tenant compte de la moindre structuration institutionnelle qui prévaut en Amérique du Nord, en général, et au Québec, en particulier, il est néanmoins possible de croire que le Comité d'harmonisation pourrait jouer un rôle de coordination / animation, et ce, tant au niveau substantiel, entre les instances provinciales, qu'au niveau fédéral. Celui-ci devrait pouvoir disposer de moyens pour ce faire, et ce, en fonction du rôle d'animation précité. Ce rôle d'animation devrait notamment pouvoir se matérialiser par l'identification ou la production de modèles de politiques internes rendus disponibles auprès des acteurs, notamment les petites et moyennes entreprises. Le droit applicable doit donc être envisagé dans le cadre de rapport internormatif entre les lois, les normes informelles et les documentations internes.

- **PROPOSITION #7 :** La mise en place d'un processus spécifique de lanceur d'alerte ne semble pas de mise sous l'égide de la LCCJTI.

- **PROPOSITION #8 :** Au regard de spécificités québécoises, une étude de la pertinence du « hacking légal » doit être envisagée tant au niveau légal, éducatif et administratif.

- **PROPOSITION #9 :** La pertinence des « bacs à sable réglementaires » doit être considérée dans des domaines où le besoin de réglementation est particulièrement utile. L'intelligence artificielle constitue un exemple où un tel besoin peut se faire sentir.

- **PROPOSITION #10 :** À l'égard de la responsabilité des intermédiaires, une approche possible consisterait à reconduire le régime actuellement prévu à l'articles 22 de la LCCJTI, mais en ajoutant des dispositions qui viendraient préciser les critères à considérer afin d'évaluer la connaissance de fait requise pour déclencher la responsabilité.
  Dans un deuxième temps, il importe de considérer la mise en place d'une instance ayant mandat d'assurer la conformité avec les conditions minimales qui seraient imposées pour le déploiement de certains dispositifs technologiques fondés sur l'intelligence artificielle. Si le Comité d'harmonisation pourrait jouer ce rôle de façon générale (voir le para. 1.2.3.2), il devra tenir compte de spécificités qui l'empêchent de traiter de certaines questions trop associées à un domaine en particulier (ex. : voitures autonomes, enseignement, etc.)
  Une telle instance de régulation pourrait prendre la forme d'un réseau de régulateurs constitué à la fois d'entités publiques et de groupes de la société civile.
  Dans les secteurs dotés d'instances de régulation, celles-ci devraient être en mesure d'intervenir en ligne lorsque cela est compatible avec le règlement efficace des conflits. Il apparaît en effet que le déploiement des technologies dans de multiples secteurs devraient être l'objet d'encadrements spécifiques.

- **PROPOSITION #11**: Les intermédiaires ne pouvant devenir responsables qu'une fois qu'ils sont informés du caractère illicite d'une activité se déroulant sur leurs plateformes, il devient nécessaire d'assurer que les instances chargées d'appliquer les lois soient dotées des outils et ressources nécessaires pour identifier de possibles activités illicites se déroulant sur des plateformes fréquentées au Québec. Une telle capacité d'identifier les activités illicites suppose d'agir de façon proactive, sans attendre de plaintes qui pourraient ne jamais venir. Mais plusieurs activités de veille pourraient être organisées en favorisant la mise en synergie des instances publiques et des groupes associatifs, par exemple, les associations de défense des consommateurs ou de protection des enfants.

- **PROPOSITION #12** : Il nous semble pertinent d'identifier dans une nouvelle disposition après l'article 22 un régime de responsabilité qui viendrait densifier les obligations à l'égard des plateformes.

- **PROPOSITION #13** : Protéger la liberté d'attention. Dans l'environnement hyperconnecté où il est si facile de diffuser, même les pires mensonges, ce n'est plus la prise de parole qui est onéreuse. C'est plutôt l'attention des auditeurs qui constitue la ressource rare et précieuse. La capacité de manipuler l'attention est à la portée de beaucoup de monde. Sur Internet, la censure opère selon des logiques différentes de celles qui prévalaient lorsque l'imprimé ou la radiodiffusion étaient les médias dominants. Pour garantir l'effectivité de la liberté de s'exprimer et de débattre, il faut non seulement lutter contre la censure dans ses manifestations classiques, il faut aussi protéger contre la manipulation et assurer l'intégrité de l'attention de ceux qui écoutent.

- **PROPOSITION #14** : Des devoirs de diligence pour les intermédiaires. Les obligations imposées aux intermédiaires pourraient être structurées en fonction du risque que représente ce qu'elles font, jumelées à leur capacité d'agir. Par conséquent, la législation devrait formuler des attentes modulées en fonction de l'importance de la plateforme pour un niveau de risque donné.

- **PROPOSITION #15** : Obligations d'évaluer et de gérer les risques. Le régime de responsabilité des intermédiaires devrait inclure une obligation pour les intermédiaires d'agir proactivement pour identifier et évaluer les risques associés aux activités qui se déroulent sur la plateforme.
  Mais il est essentiel de trouver le juste équilibre afin d'éviter que la gestion de risque soit appliquée au moyen d'exclusions arbitraires de certains contenus ou de certaines activités.
  Chaque intermédiaire assujetti à la loi serait tenu à une obligation d'identification des risques et aurait le devoir de démontrer qu'elle prend des mesures raisonnables afin de gérer les risques. L'approche reconnaît que les risques peuvent varier selon les types de plateformes et les types de service. Les risques varient également en fonction des types d'activités qui peuvent se dérouler sur une plateforme
- **PROPOSITION #16** : L'effectivité des devoirs d'évaluer et de gérer les risques suppose des garanties de vérification indépendante des processus techniques, au premier chef, les dispositifs fonctionnant au moyen d'algorithmes.

- **PROPOSITION #17 :** Retirer les dispositions relatives aux données biométriques de la LCCJTI et les transposer vers la *Loi sur la protection des renseignements personnels dans le secteur privé* ainsi que la *Loi sur l'accès aux documents des organismes publics et la protection des renseignements personnels*, d'une part, afin de regrouper au sein des mêmes documents législatifs les dispositions devant être appliquées par la Commission d'accès à l'information et, d'autre part, par souci de cohérence propre aux objets visés, à savoir des données biométriques lesquelles constituent des renseignements personnels.

- **PROPOSITION #18 :** Réviser les articles 40 à 62 LCCJTI afin de s'assurer que ceux-ci ne reflètent pas seulement les infrastructures à clé publique pour plutôt mettre de l'avant une approche associée aux identités numériques. À cette fin la norme *Digital Trust and Identity* pourrait servir d'inspiration.

- **PROPOSITION #19 :** La migration vers un système d'identités numériques renferme divers risques propres à la surveillance et au profilage des citoyens. L'approche devrait donc faire l'objet d'analyses d'incidences afin d'éviter d'importantes conséquences négatives pour la vie privée des citoyens.

- **PROPOSITION #20 :** Tel qu'il découle de ce qui précède, notre première proposition est simple : nous sommes d'avis qu'il n'est pas opportun de suivre les tendances identifiées. En effet, tel que nous l'avons soulevé, ces tendances nous semblent aller dans la mauvaise direction, c'est-à-dire, d'une part, de générer un corpus législatif « hyperspécialisé » qui risque d'échapper – tel on le voit déjà notamment en matière de poursuites pour bris de sécurité – certains risques présents ou à venir. D'autre part, une trop grande déférence au droit mou que sont les normes soulève diverses questions. Soit, il importe de tenir compte de ces normes, mais il faudrait éviter de leur donner une place prédominante et, de ce fait, abandonner à des

organismes privés une partie des compétences du gouvernement du Québec. Le Comité d'harmonisation (voir section 1.2) pourrait – tel qu'il devait le faire à l'origine – contribuer à la réflexion sur ce point.

- **PROPOSITION #21 :** Nous sommes d'avis que la rédaction des articles 25 et 26 LCCJTI mériterait une réécriture afin, d'une part, de clarifier leur portée et, d'autre part, de mieux présenter la triade disponibilité, intégrité, confidentialité et d'assurer une mise en valeur équivalente à ces trois concepts. En effet, l'article 25 s'intéresse présentement uniquement à la confidentialité, alors que l'article 26 prévoit l'obligation d'assurer la sécurité et d'en préserver l'intégrité et la confidentialité, ce qui s'avère redondant, la confidentialité et l'intégrité étant des composantes de la sécurité. Finalement, la disponibilité n'est pas citée à l'article 26. Elle n'est présente que si l'on interprète l'obligation d'« interdire l'accès [à un renseignement] à toute personne qui n'est pas habilitée à en prendre connaissance », *a contrario*, c'est-à-dire en présumant une obligation corolaire de permettre l'accès à ceux et celles qui sont habilités à en prendre connaissance. D'ailleurs, cette interprétation nous semble être la seule valable puisque, si l'on présume que le législateur ne parle pas pour rien dire, et comme interdire l'accès aux personnes non habilitées correspond à assurer la confidentialité d'une information – obligation déjà énumérée – alors on ne peut l'interpréter autrement. Cela étant, plutôt que de laisser aux tribunaux le rôle de trancher sur cette question, il nous appert pertinent de simplement clarifier le texte de ces dispositions.

  Une approche plus robuste et détaillée viendrait par ailleurs créer un système de balises auquel le législateur pourra référer dans le cadre d'autres efforts législatifs afin d'éviter les doublons (pensons ici par exemple à l'art. 6 LCCJTI et l'art. 2839 C.c.Q. en matière d'intégrité) et de s'assurer qu'il n'y a pas de contradictions entre les différents textes qui réfèrent à ces notions.

Ces propositions nous permettent de constater que préparer la LCCJTI à accompagner le Québec dans les univers technologiques d'aujourd'hui et de demain est un projet à la fois redoutable et enthousiasmant.

Outil majeur du développement des capacités de s'approprier les technologies de l'information, la LCCJTI a constitué, depuis 2001, un point de rencontre. Un lieu de dialogue entre les tenants d'une approche valorisant la continuité du droit québécois avec ses traditions civilistes et ceux qui recherchent une approche résolument ouverte à l'ensemble des technologies innovantes.

Après deux décennies où il nous a été donné de voir se consolider des façons de faire qui réservent un rôle central aux technologies de l'information, la mise à niveau de la LCCJTI se présente comme un défi aussi emballant qu'incontournable. Car c'est de la formulation des règles du jeu du monde connecté qu'il s'agit. Ce monde connecté qui est désormais le nôtre… difficile d'imaginer plus emballant défi !

BIBLIOGRAPHIE SOMMAIRE[442]

- **Lois**

Australie. (2021). *Online Safety Act*.
Canada. (2012). Loi sur la modernisation du droit d'auteur, L.C. 2012, ch. 20.
Canada. (2018). *Intimate Images Protection Act*, RSNL 2018, c I-22.
Chine. (2016). *Cybersecurity Law*.
Chine. (2021). *Data Security Law of the People's Republic of China*.
Commission européenne. (2020). Des marchés contestables et équitables dans le secteur numérique. (*Digital Services Act Package*: *Digital Service Act* + *Digital Markets Act*).
Corée du Sud. (2020). Digital Signature Act.
CNUDCI. (2022). *UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services.*
États-Unis. (1996). *Communications Decency Act* (47 U.S.C. § 230).
États-Unis. (1998). *Digital Millennium Copyright Act* (17 U.S.C. § 512).
États-Unis. (2014). *Cybersecurity Enhancement Act of 2014*.
États-Unis. (2018). California Consumer Privacy Act of 2018.
États-Unis. (2020). *AI in Government Act*.
États-Unis. *Utah Code* §§ 46-3-101.
France. (2016). *Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique*.
Québec. (1992). *Loi sur la taxe de vente du Québec*.
Québec. (2001). *Loi concernant le cadre juridique des technologies de l'information*, RLRQ, c. C-1.1.
Québec. (2017). *Loi facilitant la divulgation d'actes répréhensibles à l'égard des organismes publics*, RLRQ, c. D-11.1.
Québec. (2020). *Loi concernant le transport rémunéré de personnes par automobile*, RLRQ, c T-11.2.
Québec. (2021). *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, LQ 2021, c 25.
Québec. (2023). *Loi sur les renseignements de santé et de services sociaux et modifiant diverses dispositions législatives*, R-22.1.
Royaume-Uni. (2018). *Data Protection Act*.
Royaume-Uni. (Mars 2022). *Online Safety Bill*.
Singapour. (2018). *Cybersecurity Act*.
Union européenne. (2022). *Code de bonnes pratiques renforcé en matière de désinformation.*

- **Projets de lois ou de règlements**

Brésil. (2022). Projet de loi du Congrès brésilien #2630. *« The Fake News Law » (orig: Lei das Fake News).*
Canada. Chambre des communes du Canada. (2022). *Projet de loi C-27.*
États-Unis. (2022). *Proposal for Algorithmic Accountability Act*.
France. (2023). Projet de loi visant à sécuriser et réguler l'espace numérique.

[442] Cette bibliographie est non exhaustive et représente les sources clés qui ont été consultées lors la rédaction de ce rapport.

Québec. (2021). Projet de loi no 6 : Loi édictant la Loi sur le ministère de la Cybersécurité et du Numérique et modifiant d'autres dispositions.
Union Européenne. (2021). *Proposal for Artificial Intelligence Act*.
Union Européenne. (2022). Proposition de règlement du Parlement européen et du Conseil établissant un cadre commun pour les services de médias dans le marché intérieur (*European Media Freedom Act*).

- **Autres textes normatifs (règlements et directives)**

Canada. (2005). Règlement sur les signatures électroniques sécurisées, DORS/2005-30
Union Européenne. (1995). Directive 95/46/CE 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.
Union Européenne. (2000). Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment le commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »). JO L 178 du 17.7.2000.
Union Européenne. (2001). Directive 2001/29/CE sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information.
Union européenne. (2018). *Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (2019) (UE) 2016/679*.
Union européenne. (2019). *Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (Final document)*.
Union Européenne. (2014). *Règlement 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (dit Règlement EIDAS) .*
Union Européenne. (2016). 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.
Union Européenne. (2019). Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (refonte), PE/28/2019/REV/1.
Union Européenne. (2022). Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (DMA).
Union Européenne. (2022). Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (DSA).

- **Jurisprudence**

A.B. c. *Google*, 2023 QCCS 1167.
Allostreaming, Cass. civ. 1, 6 juillet 2017, n° 16-17.217, Bull. civ., I, n. 64.
Beaulieu c. *Facebook inc*., 2022 QCCA 1736.
Crookes v. *Newton*, 2011 SCC 47.

Dietz v. *Cypress Semiconductor Corp.*, ARB Case No. 15-017.
Gashirabake c. *Ville de Montréal*, 2023 QCTDP 16.
Gonzalez v. *Google LLC*, 598 U.S. 617 (2023).
Google Inc. v. *Society of Composer*s, 2017 SCC 34.
IO Moonwalkers, Inc. v. *Banc of America Merchant Services*, 814 S.E.2d 583 (N.C. App. 2018).
In re Mayfield, 2016 WL 3958982, No. 16-22134-D-7 (E.D. Cal. July 15, 2016).
L.D. c. *Commission de la construction du Québec*, 2017 QCCAI 34.
Lehouillier-Dumas c. *Facebook*, 2021 QCCS 3524.
Perfect 10, Inc. v *CCBill LLC,* 488 F.3d 1102 (9th Cir. 2007).
R. c. *Avanes*, 2019 ONCJ 606.
R. c. *Larouche*, 2023 QCCQ 1853.
R. c. *Veillette*, 2016 QCCQ 15192.
Sherman (Succession) c. *Donovan*, 2021 CSC 25.
Société canadienne des auteurs, compositeurs et éditeurs de musique c. *Association canadienne des fournisseurs Internet*, 2004 SCC 45.
Théberge c. *Galerie d'Art du Petit Champlain inc.*, [2002] 2 RCS 336.
Twitter, Inc. v. *Taamne*, 598 U.S. 471 (2023).
Viacom Int'l Inc. v. *YouTube Inc.,* 940 F. Supp. 2d 110 (SDNY 2013).
Warman v. Fournier, 2012 FC 803.

- **Monographies et ouvrages collectifs**

BENYEKHLEF, Karim. (2018). « Les glissements du droit à la vie privée. De Feydeau à Facebook : de la comédie de mœurs à l'économie des données », dans V. GAUTRAIS, C. RÉGIS et L. LARGENTÉ (dir.), *Mélanges Patrick Molinari*, Montréal, Éditions Thémis.

BESSEN, James. (2022). *The New Goliaths : How Corporations Use Software to Dominate Industries, Kill Innovation, and Undermine Regulation*, Yale.

BRADFORD, Anu. (2020). *The Brussels Effect : How the European Union Rules the World*, New York, OUP.

BUGE, Éric. (2021). « Les citoyens peivent-ils psrticiper à l'expression de la volonté générale en régime représentatif? », dans Mathilde HEITZMANN-PATIN et Julien PADOVANI (dir.), La participation du citoyen à la confection de la loi, Mare & Martin, Paris.

CASTETS-RENARD, Céline et Jessica EYNARD (dir.). (2022). *Un droit de l'intelligence artificielle : entre règles sectorielles et régime général*. Perspectives comparées, Bruylant, Bruxelles.

CHAMAYOU, Grégoire. (2018). *La société ingouvernable : une généalogie du libéralisme autoritaire*, Paris, La Fabrique Éditions.

FRISON ROCHE, Marie-Anne (dir.). (2016). *Internet, espace d'interrégulation*, Paris Dalloz.

GAUTRAIS, Vincent et Henry LAVILLE. (2023). « Pour une gouvernance participative des données personnelles au Québec », dans Cyril SINTEZ (dir.), *Mélanges Catherine Thibierge*, Mare et Martin, Paris.

GAUTRAIS, Vincent et Pierre TRUDEL. (2010). *Circulation des renseignements personnels et Web 2.0*, Montréal, Éditions Thémis.

GAUTRAIS, Vincent. (2012). *Neutralité technologique : Rédaction et interprétation des lois face aux changements technologiques*, Montréal, Éditions Thémis.

GIANCARLO, Frosio, (ed.). (2020). *Oxford Handbook of Online Intermediary Liability.*

HUBIN, Joël et Yves POULLET. (1998). *La sécurité informatique, entre technique et droit*, Namur, C.R.I.D.
Law and Artificial Intelligence : Regulating AI and Applying AI in Legal Practice. (2022). T.M.C. Asser Press.
LLOYD, Ian. (2020). *Information Technology Law*. United Kingdom : Oxford University Press.
MÉNISSIER, Thierry. (2021). *Innovations. Une enquête philosophique*, Paris, Hermann.
NORMAN, Donald A. (1993). *Things That Make Us Smart*, Reading, Addison-Wesley, 1993.
PROULX, Jeanne. (2011). « Méthodologie d'intégration des technologies de l'information dans le droit: l'exemple du Québec », dans Georges CHATILLON, *Droit de l'administration électronique*, Bruxelles, Bruylant.
ROCHER, François. (2010). *Guy Rocher : entretiens*, Montréal, Boréal.
ROUSSEAU, Dominique, (2021). « La figure multidimensionnelle du citoyen de la démocratie continue », dans Mathilde HEITZMANN-PATIN et Julien PADOVANI (dir.), *La participation du citoyen à la confection de la loi*, Mare & Martin, Paris.
TRUDEL, Pierre. (2012). Introduction à la Loi concernant le cadre juridique des technologies de l'information.
TYSON, Dave. (2007). *Security Convergence : Managing Enterprise Security Risk*, Burlington, Butterworth-Heinemann.
VERMEYS, Nicolas W. (2010). *Responsabilité civile et sécurité informationnelle*, Cowansville, Éditions Yvon Blais.
VERMEYS, Nicolas W. (2015). *Droit codifié et nouvelles technologies : Le Code civil*, Cowansville, Éditions Yvon Blais.
ZEMIN, Jiang. (2009). *On the Development of China's Information Technology Industry*, Elsevier Science.
ZUBOFF, Shoshana. (2019). *L'Âge du capitalisme de surveillance*, Paris, Éditions Zulma.

- **Rapports de recherche**

BENNETT INSTITUTE FOR PUBLIC POLICY DE L'UNIVERSITÉ DE CAMBRIDGE, Unger, Steve. (2019). *amsof online platforms - What can we learn from 150 years of telecoms regulation?*
CANADA, FORUM DES POLITIQUES PUBLIQUES. (2018). *Poisoning Democracy : How Canada Can Address Harmful Speech Online*.
COMMISSION CANADIENNE SUR L'EXPRESSION DÉMOCRATIQUE, *Diminuer un tort : un programme en six étapes pour protéger l'expression démocratique en ligne*. (janvier 2021).
INTERNATIONAL. ASSOCIATION INTERNATIONALE DU DROIT DE LA TECHNOLOGIE. (2021). *Responsible AI Policy Framework*.
OECD. (2019). *An Introduction to Online Platforms and Their Role in the Digital Transformation*.
QUÉBEC. (2019). Vincent GAUTRAIS, Nicolas VERMEYS, Édouard HABIB et Kenza SASSI, *Revue de littérature en matière de régulation des plateformes numériques*, Rapport final combiné à l'attention du ministère de la Justice du Canada.
QUÉBEC. (2020). Vincent GAUTRAIS, *Étude juridique sur la Loi concernant le cadre juridique des technologies de l'information* (RLRQ c C-1.1) – Mandat du ministère de la Justice du Québec.
ROYAUME-UNI, ÉCOLE D'ÉCONOMIE DE LONDRES. (2018). *Tackling the information crisis: A policy framework for media system resilience*.

ROYAUME-UNI, OFCOM. (2018). *Addressing harmful online content: A perspective from broadcasting and on-demand standards regulation*.
ROYAUME-UNI. UNIVERSITÉ COLLEGE DE LONDRES. (Juin 2019). *Algorithmic Impact Assessment : Fairness, Robustness and Explainability in Automated Decision-Making*.
SINGAPOUR. (2019). *Principles to Promote Fairness, Ethics, Accountability and Transparence in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector, Monetary Authority of Singapore.*
SINGAPOUR. (2020). *Model Artificial Intelligence Governance Framework, Info-communications Media Development Authority and Personal Data Protection Commission*.
VERMEYS, Nicolas*, et al*. (2017*).* « Étude relative à l'incidence des technologies de l'information et des communications sur la gestion de l'information dans l'administration judiciaire québécoise », étude présentée au ministère de la Justice du Québec.
WORLD BANK. (2021). *Principes sur l'identification pour le développement durable: vers l'ère numérique*.

- **Documents gouvernementaux**

AGENCE DE L'UNION EUROPÉENNE POUR LA CYBERSÉCURITÉ. (Mars 2023). *Cybersecurity of AI and Standardization*.
ASSOCIATION DES NATIONS DE L'ASIE DU SUD-EST. (2022). *ASEAN Cybersecurity Cooperation Strategy*
AUSTRALIE, CENTRE AUSTRALIEN DE CYBERSÉCURITÉ. (2017). *Strategies to Mitigate Cyber Security Incidents*.
CANADA, Comité de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes. (2018). *Democracy Under Threat: Risks and Solutions in the Era of Disinformation and Data-opolies*.
CANADA, Comité de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes. (2018). *Addressing digital privacy vulnerabilities and potential threats to Canada's democratic electoral process*.
CANADA, Comité d'examen de la législation sur la radiodiffusion et les télécommunications. (2020). *Canada's Communication Future: Time to Act*.
CANADA, Enquête conjointe sur Facebook, Inc. par le commissaire à la protection de la vie privée du Canada et le commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique. (25 avril 2019).
CANADA, Travaux du Groupe consultatif d'experts sur la sécurité en ligne mis en place par le ministère du Patrimoine canadien. (2022).
CHINE. (2017). *New Generation Artificial Intelligence Development Plan*.
COMMISSION CANADIENNE SUR L'EXPRESSION DÉMOCRATIQUE. (2021). Diminuer un tort : un programme en six étapes pour protéger l'expression démocratique en ligne.
COMMISSION EUROPÉENNE. (2020). *Assessment List for Trustworthy Artificial Intelligence*.
COMMISSION EUROPÉENNE. (2018). *Commission Recommendation on measures to effectively tackle illegal content online*.
COMMISSION EUROPÉENNE. (mai 2016). *The EU Code of Conduct on countering illegal hate speech online*.
CONSEIL DE L'EUROPE. (2021). *MSI-REF Committee of Experts on Media Environment and Reform*, *draft Recommendation on Principles for Media and Communication Governance*

DIGITAL ECONOMY PARTNERSHIP AGREEMENT (Chili – Singapour – New-Zealand) (Juin 2020).
ÉTATS-UNIS, Agence nationale des télécommunications et de l'information. (Juillet 2020). *NTIA Petition for Rulemaking to Clarify Provisions of Section 230 of the Communications Act*.
ÉTATS-UNIS, Bureau du représentant commercial. United States-Mexico-Canada Trade Fact *Sheet: Modernizing NAFTA into a 21st Century Trade Agreement*.
ÉTATS-UNIS, National Archives. (2019). *Blockchain White Paper*.
ÉTATS-UNIS, Office of Financial Regulation of Florida. (2022). *Assessment of Commerce and Regulatory Issues Presented by Blockchain Technology and Virtual Currency*.
ÉTATS-UNIS. (2023). *Discussion Draft of the NIST Cybersecurity Framework 2.0 Core*.
ÉTATS-UNIS. (2023). The White House. *National Cybersecurity Strategy*.
FRANCE, Mission Facebook. (Mai 2019). *Regulation of social networks – Facebook experiment. Submitted to the French Secretary of State for Digital Affairs*.
Free Trade Agreement between the United Kingdom of Great Britain, Northern Ireland and New Zealand (2022) (notamment le chapitre 15 sur "Digital Trade").
OBSERVATOIRE DE L'UE. (2021). *Expert Group on the Online Platform Economy: Final reports*.
PARLEMENT EUROPÉEN. (2019). *Tackling the dissemination of terrorist content online*.
PARLEMENT EUROPÉEN. (2021). *DRAFT OPINION of the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (COM(2020)0825 – C9-0418/2020 – 2020/0361(COD))*.
PATRIMOINE CANADA, Groupe consultatif d'experts sur la sécurité en ligne. (2022). *L'engagement du gouvernement en faveur de la sécurité en ligne.*
QUÉBEC, Gouvernement du Québec. (2021). *Programme Service québécois d'identité numérique.*
QUÉBEC. (2022). Conseil du statut de la femme, *Étude sur l'hostilité en ligne envers les femmes*.
ROYAUME-UNI, Bureau du commissaire à l'information. (2018). *Democracy Disrupted*.
ROYAUME-UNI, Bureau du commissaire à l'information. (2019) *Age appropriate design: A code of practice for online services: Consultation document*.
ROYAUME-UNI. Bureau central du numérique et des données. (2020). *Data Ethics Framework*.
ROYAUME-UNI, Comité de l'intelligence artificielle de la Chambre des Lords. (2018). *AI in the UK: ready, willing and able? (Background information)*
ROYAUME-UNI, Comité des communications et du numérique. (2021). *Free for all? Freedom of expression in the digital age*.
ROYAUME-UNI, Comité des normes dans la vie publique. (2017). *Intimidation in Public Life*.
ROYAUME-UNI, Comité des normes dans la vie publique. (2019). *AI and Public Life.*
ROYAUME-UNI. Commissariat à l'information. (2023). *Guidance on AI and Data Protection*
ROYAUME-UNI, Commission des affaires intérieures de la Chambre des communes. (2017). *Hate crime: abuse, hate and extremism online*.
ROYAUME-UNI, Commission des communications de la Chambre des Lords. (2019). *Regulating in a digital world*.
ROYAUME-UNI, Département du numérique, de la culture, des médias et des sports. (2019). *The Cairncross Review: a sustainable future for journalism*.
ROYAUME-UNI, Département du numérique, de la culture, des médias et des sports et de l'intérieur de la Chambre des communes. (2019). *Disinformation and "Fake News": Final Report*.

ROYAUME-UNI, Département du numérique, de la culture, des médias et des sports DCMS et Département de l'intérieur. (Avril 2019). *Online Harms White Paper*.
ROYAUME-UNI. (2022). *National Cyber Security Strategy 2022*.
SINGAPOUR. (2021). *The Singapore Cybersecurity Strategy 2021.*
SUISSE, Conseil fédéral (Gouvernement). (2021). *Intermediaries and Communication Platforms*. (Version française).

- **Articles de revues**

ALEXANDRE, Adam, Paul GRAHAM, Eric JACKSON, Bryant JOHNSON, Tania WILLIAMS, Jaehong PARK, « An Analysis of Cybersecurity Legislation and Policy Creation on the State Level », (2019) *NCS*, p. 35.
ARNER, Douglas, Janos BARBERIS et Ross BUCKLEY, « FinTech, RegTech, and the Reconceptualization of Financial Regulation », (2017) 37-3 *Northwestern Journal of International Law and Business* 371.
BENCHAYA GANS, Rachel Gans, Jolien UBACHT et Marijn JANSSEN, « Governance and Societal Impact of Blockchain-Based Self-Sovereign Identities », (2022) 41-3 *Policy and Society* 402, 403.
BLOCH-WEHBA, Hannah, «Algorithmic Governance from the Bottom Up », (2022) 48-1 *Brigham Young University Law Review 69-136.*
BRUMMER, Chris et Yesha YADAV, « Fintech and the Innovation Trilemma », (2017) 107 *GEO. L.J.* 235, à la page 291.
BURELL, J., « How the Machine "thinks": Understanding Opacity in Machine-Learning Algorithms », (2016) 3-1 *Big Data and Society* 1.
CATTAN, Jean et Joëlle TOLEDANO, « La Commission dans la mise en œuvre du DMA : citadelle assiégée ou chef d'orchestre ? », *Concurrences*, n° 3, 2022.
COHEN, Julie, « Law for the Platform Economy », (2017) 51 *University of California Davis Law Review*, 135.
EASTERBROOK, Frank H., « Cyberspace and the Law of the Horse », (1996) *University of Chicago Legal Forum* 207, 207.
FORD, Cristie and Quinn ASHKENAZY, « The Legal Innovation Sandbox », *Allard Research Commons*, 2023.
GAUTRAIS, Vincent, « Made in Canada : distinctions culturelles de la protection des renseignements personnels canadienne », (2021) *33-3 Cahiers de propriété intellectuelle* 1365.
GREENBERG, Brad A., « Rethinking Technology Neutrality », (2016) 100 *Minesota Law Review* 1495, 1498.
HABEMANN, Ryan, Jennifer HUDDLESTON SKEES et Adam THIERER, « Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future », (2018) 17-1 *Colorado Technology* LJ 37.
HSU, Tiffany, « As Deepfakes Flourish, Countries Struggle With Response », (2023) *New York Times*.
KOERNER, Katharina, « Self-Sovereign Identity as Future Privacy by Design Solution in Digital Identity ? », (2022) *IAPP*.
KONINA, Anastasia, « Banks as Delegated Regulators of Technology », (2022) 59-3 *Alberta Law Review* 753, 754.
LAIDLAW, Emily, *Mapping Current and Emerging Models of Intermediary Liability,* (2019, juin).

LESSIG, Larry, "The Law of The Horse. What Cyberlaw Might Teach", (1999) *Harvard Law Review* 501.
LIU, Sylvia, « Data Privacy, Human Rights, and Algorithmic Opacity », (2022) 110 *California Law Review* 2087.
MATTATIA, Fabrice, « Faut-il dépénaliser les hackers blancs ? », (2015) 4 *Revue de science criminelle et de droit comparé* 837.
MCCARTHY, Jonathan, « The Regulation of RegTech and SupTech in Finance : Ensuring CONSISTENCY in Principle and Practice », (2023) 31-2 *Journal of Financial Regulation and Compliance* 186-199.
OHM, Paul, « The Argument Against Technology Neutral Surveillance Laws », (2010) 88 *Tex. L. Rev*. 1685.
PÉLOQUIN, Tristan, « Quand l'intelligence artificielle vous épie à la pharmacie », (6 février 2023) *La Presse.*
REED, Chris, « Taking Sides on Technology Neutrality », (2007) 4-3 *Script-ed* 263, 266.
SAINT-ARNAUD, P. (2020, février). « Premiers contacts avec l'hypertrucage sous les traits de Bernard Derome ». *La Presse*.
TOLEDANO, Joelle, « La commission européenne, la norme et sa puissance », (2023) 2 *Pouvoirs* 83 à 95.
TRUDEL, Pierre, « Discours haineux et propos choquants », (2017) *Le Devoir*.
VERMEYS, Nicolas, « Fostering Trust and Confidence in Electronic Commerce », (2015) 20:2 *Lex-Electronica* 63, 79.

- **Articles de blogues**

BALIAN, Blanche et Laetitia GHEBALI, « CNIL : mise à jour du référentiel relatif aux dispositifs d'alerte professionnelle à la suite de la transposition de la directive européenne sur la protection des lanceurs d'alertes », 15 septembre 2023, en ligne : <https://www.dalloz-actualite.fr/flash/cnil-mise-jour-du-referentiel-relatif-aux-dispositifs-d-alerte-professionnelle-suite-de-transp>.
HANDFORTH, C. Lee, K., *Comment le numérique peut-il combler le « fossé identitaire » ?*. UNPD Blog, 19 mai 2022, en ligne : <https://www.undp.org/fr/blog/comment-le-num%C3%A9rique-peut-il-combler-le-%C2%AB-foss%C3%A9-identitaire-%C2%BB>.
SCASSA, Teresa, « Comparing the UK's proposal for AI governance to Canada's AI bill", 14 avril 2023, en ligne : <http://www.teresascassa.ca/index.php?option=com_k2&view=item&id=370:comparing-the-uks-proposal-for-ai-governance-to-canadas-ai-bill&Itemid=80>.
SUPIOT, Alain, « Le crédit de la parole », *Le grand continent*, 1er août 2022, en ligne <https://legrandcontinent.eu/fr/2022/08/01/le-credit-de-la-parole/>.
TAKHAR, Jaspreet, « UK vs Europe Approach to Regulating AI : From One Extreme to Another ? », 5 avril 2023, en ligne : <https://www.connectontech.com/uk-vs-eu-approach-to-regulating-ai-from-one-extreme-to-another/>.