L'EXPLOSION DOCUMENTAIRE : LA NORMATIVITÉ INDIVIDUELLE, NOUVEAU CENTRE DE GRAVITÉ NORMATIF[389]

Vincent Gautrais[390], Christelle Papineau[391]

[389] Cet article a été facilité par un financement du CRSH, subvention savoir, sur « La normativité individuelle ».

[390] Directeur du CRDP. Professeur titulaire, Faculté de droit de l'Université de Montréal. Titulaire de la Chaire L.R. Wilson en droit du commerce électronique. www.gautrais.com. vincent.gautrais@umontreal.ca. @gautrais

391 Candidate au doctorat en droit et intelligence artificielle sous le régime d'une cotutelle de thèse établie entre l'Université Paris I Panthéon Sorbonne et l'Université de Montréal

TABLE DES MATIÈRES

[1] Explosion documentaire. Le constat est généralisé : face à la complexité de nos sociétés, face à la quête d'une réponse sociétale aux enjeux contemporains, les normes sont de plus en plus énormes, se traduisant en plus de droit, plus de contrats, plus de documentations. Classiquement, l'expression « normes énormes » est associée au phénomène d'inflation législative à laquelle la communauté des juristes doit faire face depuis plusieurs années[392]. Nous concernant, et particulièrement au monde du numérique, nous croyons qu'elle peut également être utilisée pour décrire l'irruption d'un droit souple, à savoir, un *corpus* de règles non contraignantes qui s'inscrit en marge des dispositions légales. Cette expression permet donc aussi de décrire un phénomène d'inflation documentaire qui résulte inévitablement, de ces bulles d'inflations législatives et normatives : une disposition s'accompagne en effet souvent de sa forme documentaire d'application dans le texte qui la porte[393]. Une règle juridique, qu'elle soit de nature législative ou normative, énonce en effet souvent la forme documentaire nécessaire à son exécution.

[2] Norme : hiérarchie. Évidemment, le terme norme dispose de très nombreuses acceptions. Celle que nous allons traiter ici est celle, plutôt précise, selon laquelle la norme est la norme technique à laquelle la loi réfère souvent. En fait, dans la hiérarchie normative que nous constatons dans nos domaines d'analyse, il y a les normes législatives qui délèguent fréquemment la précision des obligations des parties à des normes techniques de différents types. Ces normes techniques délèguent à leur tour à des normes individuelles[394] que les entreprises doivent mettre en place pour se conformer. Nous évoquerons donc ce phénomène de

[392] Pour des exemples : voir Philippe MALINVAUD, «Gare aux lois émotionnelles», (2012) *RDI 585*; René SAVATIER, « L'inflation législative et l'indigestion du corps social », (1977) *Dalloz* Chron 43; Pascale DEUMIER, «Les qualités de la loi» (2005) *RTD Civ.* 93. Pascale Deumier utilise le mot « explosion » pour décrire le phénomène d'inflation législative : « ces dernières décennies, doctrine et Conseil d'État se sont accordés pour fustiger la mauvaise qualité de la loi, déclinée sous tous les angles : « inflation » profusion des lois, fragmentation, périodisation, désunification, déstructuration, explosion, déstabilisation du droit, dispersion, prolifération, désintégration du droit, mondialisation, globalisation, « dénationalisation », décentralisation, «jurisprudentialisation» du droit, multiplication des instances de production et de gestation du droit, régulations en tout genre, complexification, amplification, spécialisation, technicisation des normes, dépopularisation, professionnalisation du droit, désinformation des citoyens, décodification des grands codes »; Marie-Christine de MONTECLER, « Inflation législative : la commission des lois de l'Assemblée veut mettre le pied sur le frein », (2007) *Dalloz actualité* 1732. L'auteur rapporte les propos du Président de la Commission des lois de l'Assemblée Nationale, lequel évoque une « lutte contre le droit bavard ».

[393] Pour une liste non exhaustive d'exemples, citons le droit des successions et le testament, la vente immobilière et l'acte notarié, les connaissements maritimes en matière de transport, les amendes pour stationnement, le droit civil et les actes de naissance ou de décès, le droit civil et le contrat de mariage, les documents d'identité (passeport, permis de conduire), la procédure civile et l'assignation en justice, le contrat de bail, les mandats de perquisitions, etc.

[394] Vincent GAUTRAIS, « Normativités et droit du technique », dans Stéphane ROUSSEAU (dir.), *Juriste sans frontières, Mélanges Ejan Mackaay,* Montréal, Thémis, 2015, à la page 315.

double délégation. Dans la Partie 1, nous traiterons de ces lois qui réfèrent à la fois aux normes techniques et aux normes individuelles. Un phénomène qui n'est pas critiquable en soit – y-a-t-il lieu de faire autrement ? – mais en l'état des lieux présente des travers qu'il nous faut critiquer notamment sur le plan applicatif ; qu'il nous faut améliorer. C'est ce que nous verrons plus particulièrement dans la Partie 2 où cet usage des normes individuelles demande à être maitrisé.

1. NORMES ÉNORMES : LES NORMES DÉLÉGUÉES PAR LA LOI

[3] Plan. Dans le cadre de cette première partie, nous voulons d'abord constater le phénomène de cette délégation opérée par les lois. En effet, ce « botté en touche » est courant, particulièrement dans les domaines à saveur technique (A). Ensuite, il nous importera de montrer qu'en dépit de cette nouveauté, de cette maîtrise fort partielle quant à la manière de faire, sans doute n'y a t-il pas moyen de faire autrement (B).

1.1. ÉTAT DE L'ÉNORME DANS LA LOI : LA DÉLÉGATION CONSTATÉE

[4] Inflation constatée. Comme nous le disions plus tôt, l'inflation législative est un phénomène régulièrement dénoncé[395]. Le professeur Jacques Chevallier évoque ainsi « le volume des textes et leur rythme de production (qui) augmentent sans cesse »[396], tandis que la Professeure Catherine Thibierge rappelle, de son côté, que le Doyen Carbonnier se plaignait, déjà dans les années 1970, de ce qu'il y avait, en France, trop de textes[397].

[5] Si l'inflation législative est une réalité souvent décrite, dénoncée, plus rares sont ceux qui mettent l'accent sur le fait qu'elle s'accompagne d'une inflation documentaire. Chaque texte de loi entraîne en effet une forme documentaire d'application, voire plusieurs, si l'on garde à l'esprit qu'à

[395] Pour des exemples voir : Mistrale GOUDREAU, « Inflation législative et droit d'auteur au Canada, dans le présent », dans ce numéro ; Ejan MACKAAY, « L'inflation normative », dans ce numéro; Raymond MARTIN, «*Désinflation législative?*» (1993) *RTD civ.* 551, voir en particulier son introduction : « C'est un truisme de dire que nous souffrons d'inflation législative. Il n'est nul besoin de citer des chiffres, nous sommes tous assaillis quotidiennement par l'avalanche des textes ».

[396] Jacques CHEVALLIER, *L'État post-moderne*, 2ème édition, LGDJ, Paris, 2004. Dans la 4ème édition (2017), Jacques Chevallier parle notamment de « stock (de) textes, (d') « enflure » de textes » à la page 138.

[397] Dans son article sur la densification normative (Catherine THIBIERGE, *La densification normative* in Dalloz 2014.834) la Professeure Catherine Thibierge cite les travaux du Doyen Carbonnier. Jean CARBONNIER, *Essai sur les lois,* Defrénois, 1979. 1995 (2e ed), chap 7, L'inflation des lois, p. 307 s.

l'intérieur de chaque loi, chaque article peut s'adjoindre sa propre forme documentaire d'application. Ce phénomène apparaît en filigrane, masqué par l'attention portée exclusivement à la multiplication des règles de droit. Ainsi, parler d'énorme législatif revient inévitablement à parler, au-delà de l'explosion des règles de droit, d'énorme documentaire.

1.1.1. L'INFLATION DOCUMENTAIRE ET LA SÉCURITÉ DE L'INFORMATION

[6] La sécurité de l'information à Québec. Ce phénomène se constate souvent dans le domaine de la sécurité. Au niveau provincial, la *Loi concernant le cadre juridique des technologies de l'information*, autrement connue sous le sigle LCCJTI, répond à cinq grands objectifs énoncés dans son article 1. Parmi ces cinq objectifs, citons le fait que

> *« La (LCCJTI) a pour objet d'assurer la sécurité juridique des communications effectuées par les personnes, les associations, les sociétés ou l'État au moyen de documents quels qu'en soient les supports »*[398].

[7] Cette loi, qui compte une centaine d'articles, énonce plusieurs formes documentaires d'application[399]. Ainsi, la LCCJTI est jalonnée de mesures de sécurité, de règles, d'instructions, de moyens, de certificats et certificats d'attribut, de répertoires, de politiques, d'accréditations, de guides, de pratiques, et de rapports. La LCCJTI est aussi adossée à des verbes, tels que : documenter, noter, informer, aviser, et à des mots, comme documentation ou document. Les verbes, comme les mots, sont une forme documentaire d'application complexe à saisir pour le destinataire de la loi qui aura peut-être des difficultés pour s'y conformer. La question se pose alors de la bonne manière de se conformer aux obligations documentaires imposées par la loi. La réponse se trouve peut-être dans la loi elle-même qui délègue, à plusieurs reprises, à des normes et des standards techniques, et même, s'en remet à un comité multidisciplinaire :

> *« Pour favoriser l'harmonisation, tant au plan national qu'international, des procédés, des systèmes, des normes et des standards techniques mis en place pour la réalisation des objets de la présente loi, un comité multidisciplinaire est constitué (…) Le comité pour l'harmonisation des systèmes et des normes a pour mission d'examiner les moyens susceptibles 1) d'assurer la comptabilité ou*

[398] Loi concernant le cadre juridique des technologies de l'information, RLRQ, c. C-1.1 article 1 alinéa 1.

[399] Vincent GAUTRAIS, *La preuve technologique*, 2ième édition, LexisNexis Canada, Montréal, 2018, p. 170 et suiv.

l'interopérabilité des supports et des technologies ainsi que des normes et standards techniques permettant de réaliser un document technologique, de le signer ou de l'utiliser pour effectuer une communication ; 2) d'éviter la multiplication des procédures (…) ; 3) de favoriser la standardisation des certificats et des répertoires (…) ; 4) de garantir l'intégrité d'un document technologique par des mesures de sécurité physiques, logiques ou opérationnelles ainsi que par des mesures de gestion documentaire adéquates pour en assurer l'intégrité au cours de tout son cycle de vie ; 5) d'uniformiser les pratiques d'audit (…) ; 6) de formuler des recommandations quant à l'application de la loi (…) » [400]

[8] Il y a donc une perméabilité évidente entre la loi et les normes techniques. Cette idée est flagrante à la lecture de l'article 65 de la LCCJTI, article par lequel la loi donne au comité le droit d'élaborer « des guides de pratiques colligeant les consensus atteints sur les sujets prévus à l'article 64 »[401].

1.1.2. L'INFLATION DOCUMENTAIRE ET LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

[9] La protection des renseignements personnels au fédéral. La Loi sur la protection des renseignements personnels et les documents électroniques (dite LPRPDE ou PIPEDA) est la

« Loi visant à faciliter et à promouvoir le commerce électronique en protégeant les renseignements personnels recueillis ».

[10] Cette loi protège les renseignements personnels des citoyens. Elle entend plus précisément protéger les renseignements personnels des citoyens entrant dans le périmètre d'activité des entreprises privées relevant du palier fédéral. Cette loi est jalonnée de documents, dispersés dans les soixante douze articles qu'elle compte, et dans ses annexes : rapports, recommandations, règlements, ententes écrites, etc. Ainsi, certaines formes documentaires sont évidentes, parce qu'elles relèvent d'autres lois, parce qu'elles relèvent d'un « socle commun documentaire », à l'instar des certificats en vertu de la *Loi sur la preuve au Canada*, des ordonnances de la Cour, des délégations, des plaintes, décrets, actes notariés. Puis, il y a les formes documentaires plus difficiles à cerner, tels que les accords de conformité et les pratiques. Il y a aussi les formes documentaires énoncées par les annexes : politiques, procédures,

[400] Loi concernant le cadre juridique des technologies de l'information, RLRQ, c. C-1.1 articles 63, 64.

[401] Loi concernant le cadre juridique des technologies de l'information, RLRQ, c. C-1.1 article 65.

pratiques, lignes directrices, mesures de sécurité formulaires de demande de renseignements, procédures pour recevoir les plaintes. L'annexe 1 de PIPEDA (article 4.1 à 4.10 de ladite annexe) est en ce sens intéressante, puisqu'elle marque de manière non équivoque le point de perméabilité/ de délégation entre la loi et les normes, en l'espèce celles posées par le Code type sur la protection des renseignements personnels. En effet, l'annexe 1 est construite sur la base des 10 articles dudit code type : Ce phénomène de « copier / coller » de la norme technique par la loi illustre la délégation évidente entre les deux.

[11] La protection des renseignements personnels au Québec. Nous allons nous limiter à deux lois qui trahissent ce même phénomène d'inflation déléguée. La première est la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[402] dont le nom est suffisamment évocateur pour comprendre qu'elle protège une catégorie d'informations très précises, liées aux renseignements personnels que les organismes publics détiennent à propos des citoyens. Cette loi est jalonnée de documents d'application (répertoires, registres, ententes de collecte, ententes écrites, avis motivés, avis, demandes d'accès, mesures de sécurité propres à assurer la protection des renseignements personnels, fichiers de renseignements personnels inventaires des fichiers de renseignements personnels, fichiers confidentiels, mesures de sécurité à prendre, mesures d'accommodement raisonnables, plaintes, etc.). Il y a aussi des verbes et des mots liés à la documentation. Ce sont les mêmes que dans les textes édictés au niveau fédéral : communication, communiquer, informer, aviser, motiver, refuser. Le phénomène d'inflation documentaire, se dessine et la problématique soulevée au moment d'étudier les textes fédéraux s'entrevoit une nouvelle fois : quelle serait la meilleure manière de satisfaire à ces obligations documentaires de nature législative ? La réponse se trouve peut-être dans les articles 63.1 et 63.2 de la *Loi sur l'accès*, lesquels articles prévoient la nécessité d'édicter des « *mesures* » en vue de protéger les renseignements personnels :

> *« Un organisme public doit prendre les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables, compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support » (article 63.1)*

[402] Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ, c. A-2.1

> *« Un organisme public, à l'exception du Lieutenant-gouverneur, de l'assemblée nationale et d'une personne qu'elle désigne pour exercer une fonction, en relevant, doit protéger les renseignements personnels en mettant en œuvre les mesures édictées à cette fin par règlement du gouvernement » (article 63.2)*

C'est ici une nouvelle fois la démonstration de l'existence d'un point de perméabilité entre la loi et les normes techniques.

[12] Le second exemple est la *Loi sur la protection des renseignements personnels dans le secteur privé* qui est consacrée à la protection des renseignements personnels détenus, utilisés ou communiqués par des entreprises québécoises, dans le cadre de leurs activités commerciales et par des ordres professionnels. Cette loi est adossée à plusieurs formes documentaires d'application, disséminées dans les cent quinze articles qu'elle compte. Il est ainsi question de dossiers, registres, règles de conduite, mesures de sécurité, tout comme il est aussi question de verbes et de mots flous tels que communication, notifier, informer. La question se pose à nouveau de savoir quelle serait la meilleure manière de satisfaire à ces obligations documentaires, imposées par le législateur. La réponse est peut-être dans l'article 10 de la loi, lequel article délègue à la norme :

> *« Toute personne qui exploite une entreprise doit prendre les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support ».*

[13] Équivalent européen. Le règlement (UE) 2016/679[403], connu sous le sigle « RGPD », instrument législatif qui procède des prérogatives du Parlement et du Conseil, semblerait, de prime abord, utiliser largement ce même processus de délégation documentaire. Il est en effet adossé à des politiques, à des procédures, mesures, des demandes, des mesures appropriées, des notifications, des communications, des mesures et protections techniques et organisationnelles appropriées, des mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel, des examens, des analyses d'impact[404], des

[403] 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.

[404] Règlement (UE) 2016/679, à la section 3.

certifications[405], des autorisations écrites, des contrats, des registres d'activités, des codes de conduite[406], des règles d'entreprises contraignantes, des lignes directrices, des recommandations, des bonnes pratiques, des rapports. Puis, il y a les verbes ou mots flous : procéder à toute communication, fournir, communiquer, notifier, documenter, description.

[14] Le constat est le même que pour les lois fédérales et provinciales précitées et la question que nous nous sommes déjà posée revient : si la documentation d'origine législative est abondante, quelle serait la meilleure manière de s'y conformer ? La réponse à cette question se trouve peut-être à nouveau du côté « des mesures techniques et organisationnelles appropriées », « des politiques appropriées en matière de protection des données », « un code de conduite » (pour ne citer qu'eux) lesquels instruments sont une délégation de la loi à une normativité alternative. L'article 24 du RGPD illustre cette délégation de la loi à la norme :

> *« Compte tenu 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 met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et actualisées si nécessaire »[407].*
>
> *« Lorsque cela est proportionné au regard des activités de traitement, les mesures visées au paragraphe 1 comprennent la mise en œuvre de politiques appropriées en matière de protection des données par le responsable du traitement »[408].*
>
> *« L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou de mécanismes de certification approuvés comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des obligations incombant au responsable du traitement »[409].*

[405] Règlement (UE) 2016/679, en particulier à l'article 42.

[406] Règlement (UE) 2016/679, en particulier à l'article 40.

[407] Règlement (UE) 2016/679, article 24 alinéa 1.

[408] Règlement (UE) 2016/679, article 24 alinéa 2.

[409] Règlement (UE) 2016/679, article 24 alinéa 3.

1.1.3. L'INFLATION DOCUMENTAIRE ET LE DOMAINE DE LA SANTÉ

[15] ***Sécurité.*** Prenons le pouls de cette inflation documentaire en partant d'un premier constat dans le domaine de la santé où le corpus de lois applicables en la matière est énorme[410] : *Loi sur la protection des renseignements personnels et les documents électroniques, Loi sur les services de santé et les services sociaux*[411] et la *Loi sur l'assurance maladie*[412], sans oublier le *Code de déontologie des médecins*[413].

[16] Inflation documentaire au Québec. Intéressons-nous à la *Loi sur les services de santé et les services sociaux.* Cette loi, qui compte six cent vingt-deux articles, est adossée à plusieurs dizaines de formes documentaires d'application, à l'instar des politiques, des dossiers, fichiers, index locaux, demandes d'accès, mesures, engagements de confidentialité, registres, des règlements, des procédures, procédures d'examen des plaintes, des ententes, des bilans (notamment du commissaire régional aux plaintes), des rapports, des dossiers, des conclusions, des compléments d'examen, des demandes de révision, des avis écrits (semblables à des accusés de réception), des observations, rapports dédiés aux motifs des plaintes, des recommandations (formulées par des comités), des plans d'organisation, des protocoles, des propositions. Puis, il y a les verbes : informer, et sa déclinaison à la forme passive « être informé », communiquer, aviser, recommander. Et enfin, il y a les mots : communication, information.

[17] ***HIPAA Privacy Rule*** **et** ***HIPAA Security Rule*****.** HIPAA est l'acronyme qui permet de citer plus facilement la loi fédérale américaine connue sous le nom de The Health Insurance Portability and Accountability Act of 1996. HIPAA est une loi qui a vocation à protéger la vie privée et certaines informations de santé des citoyens américains. HIPAA a subi deux déclinaisons : la première est connue sous l'expression HIPAA Privacy Rule, tandis que la seconde est connue sous l'expression HIPAA Security Rule. Nous traiterons ces deux déclinaisons ensemble.

410 Pour en savoir plus, Vincent GAUTRAIS et Catherine RÉGIS, « Cybersanté : les tentatives juridiques pour objectiver un domaine en pleine effervescence », Vincent GAUTRAIS, Catherine RÉGIS et Laurence LARGENTÉ, *Mélanges Molinari*, Montréal, Éditions Thémis, 2018, pp. 195-226.

411 Loi sur les services de santé et les services sociaux, RLRQ, c. S-4.2.

412 Loi sur l'assurance maladie, RLRQ c A-29.

413 Code de déontologie des médecins, RLRQ c M-9, r 17.

[18] HIPAA Privacy Rules a vocation à protéger les dossiers médicaux des citoyens américains et les données en santé les concernant. Son champ d'application s'étend à toute les professions œuvrant dans le domaine médical. HIPAA Security Rule a, de son côté, vocation à protéger les données en santé de nature électronique. Les articles dédiés à HIPAA sont nombreux, ils se comptent en dizaines, et offrent, à l'instar des textes canadiens et québécois que nous avons étudié jusqu'à présent, la même quantité de formes documentaires d'application. Si certaines formes semblent évidentes (à l'instar des complaints), d'autres formes documentaires semblent moins aisées en terme de compréhension (tels standards, requirements, implementation specifications, policies, procedures, documentation, compliance reviews, preliminary reviews, compliance reports, operating rules, guidelines, business rules, implementation specifications). Les formes documentaires s'annonçant sous la forme de verbes sont encore une fois très présentes. Parmi toutes ces formes documentaires, les plus récurrentes sont les politiques et les procédures.

1.2. ÉTAT DE L'ÉNORME DANS LA LOI : LA DÉLÉGATION OBLIGÉE

[19] Pas le choix ! Cette délégation législative, nous le verrons dans la partie 2, est source à de nombreuses critiques. Ceci dit, il ne s'agit pas de « jeter le bébé avec l'eau du bain » cette approche très processuelle étant sans doute la seule en mesure de gérer la complexité inhérente au numérique.

1.2.1. UNE INFLATION DOCUMENTAIRE POUR GÉRER LES CHANGEMENTS

[20] Gérer l'information comme un actif. L'inflation normative et documentaire décrites sont particulièrement vraies en matière de sécurité de l'information et de vie privée. Dans ces domaines, et au-delà de cette délégation, on peut identifier plusieurs raisons qui militent pour cette explosion. D'abord, l'information est considérée depuis plusieurs années comme un actif qui mérite, à ce titre, protection[414]. Elle se décline sous des formes différentes, c'est-à-dire verbale ou écrite et se matérialise

[414] Voir en particulier l'article 0.1 alinéa 3 de la norme ISO/CEI 27002:2013 (F) : "la valeur de l'information dépasse les mots, les chiffres et les images : la connaissance, les concepts, les idées et les marques sont des exemples de formes d'information immatérielles. Dans un monde interconnecté, l'information et les processus, systèmes et réseaux qui s'y rattachent, ainsi que le personnel impliqué dans son traitement ses manipulations et sa protection, sont des actifs précieux pour l'activité d'une organisation, au même titre que d'autres actifs d'entreprise importants, et par conséquent, ils méritent ou nécessitent d'être protégées contre les divers risques encourus"; voir également l'article 3.2.2 de la norme ISO/IEC 27000:2016 (E) : « Information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected ».

par l'intermédiaire de supports papier, informatique, audio, vidéo. Elle revêt des « costumes » tantôt juridiques, et comptables, tantôt commerciaux et financiers.

[21] Gérer l'information comme un risque. L'information représente aussi un risque[415]. Elle est en permanence source de risque pour les organisations qui, tour à tour, la génèrent, la collectent et en sont destinataires (lorsqu'elles sont produites par leurs partenaires). L'information a toujours existé et les risques ont eux aussi toujours existés. Il y a toujours eu des menaces, en interne, émanant des salariés de l'organisation[416]. Les menaces venant de l'extérieur ont elles aussi toujours existées[417]. Il y a enfin toujours eu des risques de détériorations et pertes de l'information en raison de cas de force majeure : météorologie défavorable, incendies, inondations…[418]. L'apparition de l'Internet et du web a tout changé. Ce n'est tant l'Internet ou le web, mais plutôt les risques qu'ils génèrent en terme de vulnérabilité, qui ont obligé, et obligent les organisations à repenser leurs rapports avec les masses d'informations qu'elles génèrent quotidiennement, mensuellement et annuellement.

[22] Gérer la hausse de la délinquance informationnelle. La prise de conscience vis-à-vis de la protection de l'information se démultiplie encore à mesure que les cyber-attaques augmentent, *a fortiori* quand le piratage avait pour cible des administrations (les pirates touchent alors

415 Voir l'article 3.4 de la norme ISO/IEC 27000:2016 (E).

416 Jean-Emmanuel ray, Droit social 2013.111. Pour l'auteur, « (…) avec son brave Iphone personnel, un collaborateur indélicat peut charger au bureau des méga-octets de données, ou tout simplement photographier voire filmer des pages d'écran où apparaissent des informations ou des dessins confidentiels sans que le service informatique ne puisse constater un quelconque téléchargement, transfert de données ou tirage papier (…) Une pensée émue donc pour le salarié qui, au millénaire dernier, partait à la concurrence avec 12 kilos de documents confidentiels discrètement photocopiés, petit à petit, soir après soir depuis un an ; une clé USB chargée en deux minutes lui permet aujourd'hui de partir avec l'équivalent de 12 tonnes ». Pour un autre exemple, voir : Éloïse Gratton et Frédérick Néron qui évoquent, plus simplement, les cas d' « employé qui oublie un document confidentiel » et « l'envoi d'un courriel à un destinataire erroné » dans Éloïse Gratton et Frédérick Néron, « *Bris de sécurité informationnelle : étape à suivre et gestion des risques* » (2014), Développements récents : les 20 ans de la Loi sur la protection des renseignements personnels dans le secteur privé (2014), n°392, Yvon Blais, 2014.

417 Pour des exemples, voir : Marie Anglade, Protection des données, Jurisport 2018 numéro 188 p 47 (à propos du vol d'ordinateur portable dans un train alors que cet ordinateur contient les données personnelles des adhérents à un club sportif); voir l'affaire Langevin aux Etats-Unis. L'affaire est brièvement relatée dans l'article de André R. Bertrand « *une donnée* », Informations, données, bases de données, Chapitre 201, section 201.15, Dalloz Action Droit d'auteur 2010 (dans cette affaire, un ancien employé de la Banque Centrale des Etats-Unis avait utilisé un code lui permettant de consulter une information, dans le but de le réutiliser auprès de son nouvel employeur).

418 Voir en ce sens l'article 11.1.4 de la norme ISO/CEI 27002:2013 (F) et à titre d'illustration les ouragans HARVEY, IRMA, JOSE et MARIA qui ont dévasté certains états américains en 2017, et le bassin des Caraïbes.

aux fonctions vitales d'un État)[419], des entreprises d'importance (les pirates touchent à des intérêts économiques) ou des milliers de citoyens[420]. La prise de conscience est d'autant plus importante quand l'attaque ciblait simultanément des entreprises d'envergure et des administrations[421].

[23] Gérer la hausse des traitements de données personnelles « problématiques ». Il serait faux de croire que la délinquance informationnelle ne prend la forme que de cyberattaques diligentées contre des administrations ou des sociétés commerciales. Les évènements liés aux affaires *Cambridge Analytica*, et *Leave.UE* ont montré que les informations pourraient être utilisées comme moyens d'influence sur le vote des citoyens. Cette information qui semblait *a priori* si anodine et empreinte d'un caractère si gentiment ludique est alors devenue une arme de nature constitutionnelle pouvant manipuler les intentions de vote des électeurs-utilisateurs.

[24] Hausse de la diligence. Si dans le domaine du numérique, les années 1990-2000 sont aujourd'hui encore associées à un certain laxisme du point de vue de la responsabilité des organismes[422], force est de constater que la tendance s'est inversée face à cette délinquance informationnelle. Le législateur a élargi le champ d'application de la responsabilité des organisations, en témoigne le RGPD et la fameuse sanction de l'article 83 qui peut amputer « jusqu'à 4% du chiffre d'affaire annuel mondial total de l'exercice précédent »[423]. Cette hausse de la diligence se traduisent inévitablement par « plus » de documents au sein des organisations : plus de documents exigés par la loi, ceux listés dans la première partie, et plus de documents issus de la normativité technique, pour s'adapter à la loi, l'appliquer, s'y conformer et prouver en cas de problème.

[419] Le Rapport émis par la Sécurité publique du Canada indique que « Le gouvernement du Canada empêche en moyenne plus de 600 millions de tentatives quotidiennes d'identification et d'exploitation des vulnérabilités de ses systèmes et réseaux » Sécurité Publique Canada, *Évaluation horizontale de la Stratégie de cyber sécurité du Canda,* Rapport final du 29 septembre 2017 à la page 20.

[420] Voir par exemple la cyberattaque ayant ciblé la société Equifax.

[421] Pour un exemple, voir la propagation du virus Peyta, en 2017, en Ukraine, Voir également la cyber attaque dont l'édition des Jeux Olympiques de 2018 aurait été victime quelques heures avant la Cérémonie d'ouverture.

[422] On peut notamment penser au régime d'exonération de responsabilité qui prévaut dans la plupart des juridictions relativement aux intermédiaires techniques. Voir par exemple l'article 22 de la Loi concernant le cadre juridique des technologies de l'information.

[423] Règlement (UE) 2016/679, article 83 alinéa 5.

[25] Objectivation de la diligence. Les tentatives d'intrusion tout comme les attaques « réussies » ou les manipulations de données par les organismes qui en ont la garde, sont des évènements qui ont placé les États, les sociétés commerciales et autres organisations sous une épée de Damoclès : tout peut arriver, à n'importe quel moment, sous des formes variées mais surtout de plus en plus astucieuses. Les organisations doivent être mesure de prouver leur diligence, de rendre des comptes publiquement à toute personne qui en ferait la demande. A l'instar de l'affaire *Equifax*... On sait combien cela est important à une époque où les relais médiatiques sont nombreux et les tribunes d'expression (pour faire part de son mécontentement) diversifiés. Dans cette époque de la réputation, de la recherche de la vérité et du penchant pour la bonne foi, l'une des manières de prouver sa diligence serait encore de démontrer son allégeance à des normes complémentaires aux lois. Cette manière de faire est donc inhérente aux matières techniques, de surcroît lorsque celles-ci présentent un certain degré de complexité[424].

1.2.2. UNE INFLATION DOCUMENTAIRE IMPOSÉE PAR LE DROIT

[26] Les conditions sont réunies pour qu'il y ait densification normative, ce phénomène théorisé par Catherine Thibierge au début des années 2000[425] et qui prend la forme de ce que nous appelons « délégation constatée », à savoir une délégation du législateur à des standards techniques et, conséquemment, à une normativité individuelle. Les conditions sont donc réunies pour qu'il y ait, en conséquence, une inflation documentaire.

[27] Objectivation type « Facebook ». Si cette densification normative s'explique par ce phénomène de délégation législative, elle trouve en réalité une origine beaucoup plus profonde, à savoir, dans ce désir qu'a la société de vouloir garder la main sur les activités commerciales qui s'opèrent sans contrôle, à l'instar de *Facebook*. Sous couvert d'un réseau social qui ne voudrait que connecter les personnes entre elles, il y a en réalité, une activité commerciale « souterraine », obscure, directement liée à l'information que les utilisateurs disséminent à chacun de leur passage sur le réseau : *likes*, commentaires, *post* et autres photos sont

[424] Vincent GAUTRAIS, « Preuve et développement durable : objectivation du droit par la normativité individuelle », dans Vincent GAUTRAIS et Mustapha MEKKI, *Preuve et développement durable*, Montréal, Éditions Thémis, 2016, pp. 43-74.

[425] Catherine THIBIERGE, La densification normative in Dalloz 2014.834

autant de matières premières extraites, comme dans une mine, puis commercialisées. Achetées par des courtiers (*data brokers*) ou des analystes, elles servent autant à détecter la tendance générale qu'à prédire le comportement d'un seul. L'on comprend l'intérêt des acheteurs de données et l'on comprend aussi la prise de conscience des utilisateurs. Une prise de conscience qui s'est accrue avec le scandale *Cambridge Analytica*, avec la possible ingérence russe dans les élections présidentielles américaines de 2016 et avec la possible immixtion dans le vote du *Brexit*. S'il y a eu « le » scandale *Cambridge Analytica*, il y a aussi eu, quelques mois auparavant, l'affaire *Equifax* : l'affaire portait sur le vol de données personnelles liées à l'identité d'au moins cent quarante-cinq millions d'américains (« *noms, numéros de sécurité sociale, dates de naissance et dans certains cas, numéros de permis de conduire* »[426]). La Commission des finances du Sénat américain s'était saisie de l'affaire en sollicitant des explications du dirigeant de l'entreprise[427]. Une pratique qui sera reprise au moment du scandale *Cambridge Analytica*, le Congrès américain ayant auditionné Mark Zuckerberg. Au travers de ces auditions de plus en plus fréquentes, le pouvoir législatif fait la démonstration que le curseur des obligations de nature juridique tend à investir la sphère de la diligence. Le Congrès auditionne et requiert d'avoir des réponses juridiques claires à des problématiques juridiques claires. La réponse des dirigeants passe par leur capacité à prouver, c'est-à-dire à « verser au débat » les bons documents d'exonération de toute responsabilité, ceux qui démontreront que les meilleurs efforts ont été faits. De façon identique, les instances britanniques[428] et européennes[429] évaluent en ce moment de la même manière si une responsabilité de l'entreprise, ou d'autres entités, est à dégager de cette affaire.

---

[426] Agence France Presse Washington, *Equifax : 145, 5 millions d'Américains touchés par le piratage, dû à une faille non corrigée*, édition en ligne du 2 octobre 2017 http://www.lapresse.ca/techno/actualites/201710/02/01-5138661-equifax-1455-millions-damericains-touches-par-le-piratage-du-a-une-faille-non-corrigee.php

[427] Lettre du Comité des finances du Sénat du 11 septembre 2017 adressée à Richard Smith, consultable en ligne https://www.finance.senate.gov/imo/media/doc/9.11.17%20Hatch,%20Wyden%20Request%20Information%20on%20Equifax%20Breach_Redacted.pdf (consultée en septembre 2018).

[428] Voir en ce sens la lettre que le « Digital, Culture, Media and Sport Committee » a adressé, par l'intermédiaire du parlementaire Damian Collins, à Facebook UK pour convoquer le dirigeant américain, le 24 mai 2018, https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/180501-Chair-to-Rebecca-Stimson-Facebook-re-oral-evidence-follow-up.pdf https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/news/fake-news-facebook-correspondence-17-19/ (consultés en novembre 2018).

[429] Le Parlement européen a programmé « une série de trois auditions », les 4 juin 2018, 25 juin 2018 et 2 juillet 2018 http://www.europarl.europa.eu/news/fr/press-room/20180625IPR06510/deuxieme-audition-facebook-cambridge-analytica ;http://www.europarl.europa.eu/news/fr/press-room/20180530IPR04607/facebook-cambridge-analytica-les-deputes-poursuivent-leur-examen (communiqués consultés en novembre 2018). Ces communiqués de presse du Parlement rappellent que ces auditions ont été « organisées par la commission des libertés civiles, en association avec les commissions de l'industrie, des affaires constitutionnelles et des affaires juridiques ».

[28] L'inflation documentaire et le législateur. En pratiquant l'audition de dirigeants, le législateur envoie un signal fort en matière « d'*accountability* documentaire » : le législateur veut des preuves (preuves des consignes données aux salariés en interne dans le « tous les jours » de l'organisation, preuves de la « bonne réaction » au moment d'un incident affectant l'information). Il rappelle ainsi que la loi prend la forme de certains documents pour s'exonérer de sa responsabilité et souligne en même temps le potentiel des documents issus des normes techniques pour documenter la façon de considérer la valeur de l'information en tant qu'actif, la façon de gérer le risque et de réagir face au risque devenu réalité. Le dirigeant doit prouver dans le champ d'application de la loi et être en mesure de compléter ces documents d'origine légale par des documents élaborés en interne sur la base des normes techniques. Le phénomène d'inflation trouve ici son explication.

[29] L'*accountability* est une notion purement juridique dont la gestion dans le quotidien d'une organisation est en réalité beaucoup trop technique pour être appréhendée de manière satisfaisante par le législateur. Ainsi, la délégation que celui-ci opère vers la norme technique créé inévitablement de l'inflation documentaire générées par trois sources distinctes : lois, normes techniques et normes individuelles. En agissant de la sorte, le législateur lui-même montre que cette quête de l'efficacité réside dans la documentation technique à laquelle la loi renvoie : les organismes producteurs de normes techniques ont une réputation : ISO, AFNOR, etc. et s'annoncent comme un label, une marque de confiance. En prouvant sa conformité à ces labels normatifs, parce qu'ils ont une réputation, en plus de sa diligence législative, une organisation incriminée optimise ses chances de démontrer qu'elle avait bien agit.

2. NORMES ÉNORMES : LES NORMES APPLIQUÉES DANS LA NORME INDIVIDUELLE

[30] Suspicion nécessaire. Sauf exception, les juristes n'ont pas l'habitude de s'intéresser aux normes techniques. Et c'est bien dommage… du fait de leur prolifération, de leur contenu substantiel, il importe d'appréhender ces textes, et ce, même s'ils disposent parfois d'une teneur moindrement accessible. L'intérêt à les lire tient aussi au fait que malgré leur nombre, on peut constater des différences mais aussi

beaucoup de similitudes qu'il importe de connaître. Également, il importe d'avoir un regard critique sur ces textes qui sont adoptés sans que l'on ne sache toujours par qui et comment. Et si ces textes, parfois, bénéficiaient à des groupes d'intérêt ?

2.1. ÉTAT DE L'ÉNORME DANS LA NORME : LA CACOPHONIE DOCUMENTAIRE

[31] Il y a un schéma qui permet de résumer les délégations objets du présent article : c'est le schéma dessiné dans notre introduction qui montre la loi déléguant à la norme technique (ISO, AFNOR, etc.) laquelle norme se transforme en norme individuelle (« politiques, procédures, codes, lignes directrices internes »[430]) pour finalement se fondre dans une organisation. La sentence tombe : ce schéma est révélateur d'une situation de cacophonie documentaire puisque les sources documentaires sont multiples.

2.1.1. CACOPHONIE NORMATIVE AU REGARD DE ISO 27000

[32] Intégration inter-normative (1). Si la sécurité de l'information est intégrée dans plusieurs lois fédérales et provinciales, elle est aussi relayée par plusieurs normes, dont celles de la famille ISO/CEI 27000 et suivantes. La sécurité de l'information repose donc sur des lois complétées par des normes. Cette architecture est l'illustration parfaite d'un thème qui a autant besoin du pouvoir de contrainte de la loi que de compléments normatifs pour tendre vers une protection efficace et efficiente. La loi est capable d'obtenir, dans son principe, le respect des règles de sécurité par le jeu de l'*accountability* et la norme technique transformée par la suite en norme individuelle s'entrevoit comme un instrument d'application dans le quotidien d'une organisation.

[33] Intégration inter-normative (2). Si la loi énonce des formes documentaires auxquelles il est impossible de se soustraire, force est toutefois de constater qu'elle n'explicite pas la manière dont la documentation doit se matérialiser : le législateur s'en tient au conseil documentaire. Cette absence de précision résonne comme un aveu de faiblesse de la part de la loi ; comme une autorisation implicite à se tourner vers le droit souple pour y trouver de l'aide. Dans ce contexte, la norme labellisée ISO apparaît comme une solution documentaire prêt à

[430] Voir Vincent GAUTRAIS, « Révolution numérique et quête de davantage de garanties normatives : les algorithmes sous contrôle » dans Catherine THIBIERGE, *La garantie normative*, à paraître.

l'emploi. C'est une option salvatrice pour une organisation qui veut bien faire pour documenter la manière dont elle protège l'information dont elle est gardienne. Chaque article ISO souligne la forme documentaire idéale et les grandes lignes d'un contenu correspondant aux critères communément admis. Comme le soulignent Vincent Gautrais et Pierre Trudel :

> *« les normes informelles disposent souvent d'une capacité expressive qui permet d'objectiver les silences (…) du droit formel »*[431].

[34] ISO 27000 et suivantes : la famille la plus connue. Les normes ISO/CEI sont des préconisations techniques, élaborées à un niveau international. Elles offrent des solutions pratiques aux problèmes récurrents qu'une organisation est susceptible de rencontrer dans le cadre de ses activités[432]. La famille des normes ISO/CEI 27 000 est, dans ce paysage normatif, une famille de normes récente, consacrée aux techniques de sécurité de l'information Cette famille cartographie les risques menaçant une organisation, que ces risques soient de nature « *accidentel (ou) délibéré* »[433]. L'objectif de cette famille de norme est de proposer, sous la forme d'un catalogue, des solutions optimums de protection, via l'élaboration d'un système de management de la sécurité de l'information et son maintien en état de fonctionnement. Les normes de cette famille relèvent, à l'instar de toutes les normes ISO, du droit souple c'est-à-dire de propositions non contraignantes : les organisations sont ainsi libres de les appliquer ou de les écarter[434]. Toutefois, un refus

[431] Vincent GAUTRAIS et Pierre TRUDEL, « mondialisation et Internet au Québec », dans Travaux de l'Association Henri Capitant des amis de la culture juridique française, La mondialisation, Journées allemandes, Bruylant et LB2V, 2016, à la page 910.

[432] En ce sens, voir : Magali Lanord FARINELLI, La norme technique : une source du droit légitime ? RFDA 2005.738. L'auteure reprend la définition du terme normalisation donnée par le décret n 84-74 du 26 janvier 1984 :« La normalisation a pour objet de fournir des documents de référence comportant des solutions à des problèmes techniques et commerciaux concernant les produits, biens et services qui se posent de façon répétée dans des relations entre partenaires économiques, scientifiques, techniques et sociaux ». Le décret auquel l'auteure fait référence a été abrogé par le décret n 2009-697 du 16 juin 2009 et remplacé dans les termes suivants par ce même décret (article 1) :« La normalisation est une activité d'intérêt général qui a pour objet de fournir des documents de référence élaborés de manière consensuelle par toutes les parties intéressées, portant sur des règles, des caractéristiques, des recommandations ou des exemples de bonnes pratiques, relatives à des produits, à des services, à des méthodes, à des processus ou à des organisations ».

[433] ISO/CEI 27002:2013 (F), article 0.1, alinéa 4.

[434] Voir Vincent GAUTRAIS, « Normativités et droit du technique », dans Stéphane ROUSSEAU (dir.), Juriste *sans frontières, Mélanges Ejan Mackaay,* Montréal, Thémis, 2015, à la page 324. L'auteur présente le « (…) droit mou comme une normativité de suggestion ; dénuées d'aucune contrainte, ces normes sont du non-droit, suggestif, mais non contraignant ».

d'application ne les dédouanera pas de mettre en place des mesures de protection de l'information en vertu du droit commun[435].

[35] Application des normes. Quand une organisation décide d'appliquer les préconisations de cette famille de normes, c'est le prélude d'une certaine « *cacophonie* » normative. Dans une démarche optimale d'adhésion, l'organisation qui se soumet auxdites recommandations, devrait considérer comme un tout, le contenu des vingt normes, dont certaines peuvent faire jusqu'à cent pages[436]. A l'intérieur de cet ensemble, chaque norme opère des renvois réguliers, d'importance variables, à d'autres normes, appartenant soit à la famille des ISO/CEI 27 000[437], soit à d'autres normes ISO[438]. Ces renvois obligent l'organisation à pratiquer une lecture croisée entre le texte originellement à l'étude et le texte de renvoi (quand ce texte de renvoi ne procède pas lui-même à d'autres renvois). En conséquence, suivre consciencieusement chaque préconisation et ses renvois peut très vite conduire à une inflation normative et à un débordement documentaire, au sein de la structure, par la création de nouvelles politiques, procédures, mesures, plans et autres journaux qui viennent concurrencer une normativité déjà largement inflationniste comme nous aimons le répéter[439].

[435] Le refus d'application des normes ISO/CEI 27 000 n'est pas toujours volontaire, il peut relever d'une incapacité à payer le prix des normes : le coût global de l'accès à la famille des normes ISO/CEI 27 000 est d'environ 4 540 dollars canadiens (20 normes à 227 dollars l'unité) ou 3 100 euros (20 normes à 155 euros l'unité). Ce montant évince automatiquement les organisations qui ne sont pas en mesure d'en payer le prix, en particulier les petites structures générant des chiffres d'affaire modestes (autoentrepreneurs, *start-up* démarrant leur activité…). Sur ce point, voir : Nicolas Vermeys, qui évoque l'idée d'une « *industrie des normes* » (Nicolas Vermeys , Responsabilité civile et sécurité informationnelle , Cowansville, Éditions Yvon Blais, 2010, p. 103); Vincent GAUTRAIS et Pierre TRUDEL, « Mondialisation et Internet au Québec », dans Travaux de l'Association Henri Capitant des amis de la culture juridique française, La mondialisation, Journées allemandes, Bruylant et LB2V, 2016, à la page 910 (Les auteurs expliquent que « Ces normes de l'industrie se multiplieraient donc à cause des argents qu'elles généreraient auprès des communautés qui les élaborent ou certifient leur application »). Puis, il y a les renvois à d'autres normes ISO que les normes de la famille ISO/CEI 270000 et suivantes peuvent proposer. Ces renvois ont un coût qui peut, en fonction des choix qu'une organisation fera, se greffer aux chiffres que nous venons d'évoquer.

[436] La norme ISO/CEI 27002:2013 (F) compte 98 pages.

[437] Par exemple, la norme ISO/IEC 27018:2014 (E), consacrée à la protection des données personnelles, doit être par exemple être lue de concert avec la norme ISO/CEI 27002:2013.

[438] Par exemple, la norme ISO/CEI 27001:2013 (F) renvoie à la norme ISO 31000 :2009 tandis que la norme ISO/CEI 27002:2013 (F) renvoie à la norme ISO/CEI 29100 en matière de protection des données à caractère personnel dans les systèmes informatiques.

[439] Pour le cas des entreprises voir : le Club des Juristes, *3 questions à Nicolas Molfessis sur l'inflation législative et l'office de la loi*, l'actualité au prisme du droit, 10 juillet 2017, consultable en ligne http://blog.leclubdesjuristes.com/3-questions-a-nicolas-molfessis-linflation-legislative-loffice-de-loi/ « Le trop plein de lois est dénoncé de toutes parts depuis plus d'un quart de siècle (en France). La France souffre d'un étouffement normatif qui sclérose l'activité humaine, provoque un sentiment d'angoisse face à la norme, réfrène les initiatives et les envies. Le droit, qui devrait libérer les énergies et façonner une société meilleure et plus sûre, devient souvent oppressant. Chacun le subit dans sa vie quotidienne : face aux règles qui pèsent sur nous, nous étouffons (…) Les entreprises en font ainsi l'amère expérience, surtout les (Petites et Moyennes Entreprises) qui n'ont pas la possibilité, comme les grandes entreprises, d'être dotées de cohortes de juristes pour faire face à la norme », Pour le cas des associations voir: Jean Dalichoux, *Quelques repères dans le maquis des textes normatifs,* JA 2009, n 407 p 29 « Face à cette abondance de textes, les associations quelle que soit leur taille, peuvent être confrontées à des difficultés d'interprétation ou des oublis préjudiciables à leur bon fonctionnement ».

[36] Politiques, procédures, mesures, etc.: oui, mais quelles définitions ? Les évolutions numériques sont « maîtres » du jeu puisqu'elles imposent une cadence que le législateur ne peut pas suivre. En proposant de déléguer le principe générique d'*accountability* à la normativité souple, le législateur sait qu'il renvoie le destinataire vers un cadre adapté autant à ses besoins qu'aux évolutions numériques. D'autant que les mises à jour sont régulières. Les textes législatifs que nous avons étudiés, qu'ils soient canadiens, européens ou états-uniens, citent à plusieurs reprises les formes documentaires d'origine normative que sont les politiques, les procédures et les mesures. Si les législateurs y réfèrent pêle-mêle, sans plus d'attention ni d'intérêt en terme de définition, il faut toutefois savoir que ces normes sont définies, hiérarchisées entre elles et qu'il y a un code de valeur qui les ordonnance. La politique est l'ensemble des consignes exprimées/formulées par le plus haut niveau de direction d'une organisation[440]. La procédure est une application plus concrète des politiques puisque son objectif est de traduire en langage opérationnel les principes posés par les politiques. Ainsi, l'on comprend que la politique a une valeur supérieure à la procédure, laquelle procédure est placée au delà des mesures et autres directives. Cet agencement hiérarchisé s'observe particulièrement bien dans le cadre de la famille des normes ISO 27 000

> *« (les normes ISO 27001 et ISO 27002) établissent une pyramide des normes composée de plusieurs étages. Tout en haut existe en premier "une" **politique** suprême, au singulier, émanant de la direction de l'institution. Elle édicte les objectifs de l'organisation et doit faire l'objet d'une communication soutenue en son sein (…). En dessous de ce texte, il y a, en deuxième lieu, des **politiques**, au pluriel cette fois (…). Ces politiques réfèrent à une série d'obligations fort nombreuses portant, sans prétention d'exhaustivité, sur les définitions, les responsabilités, les processus de traitement, le contrôle d'accès, la classification, la sécurité physique, les transferts d'information, et de tant d'autres choses encore (…). En troisième lieu, il est en effet possible d'identifier les **procédures** qui viennent préciser les précédents. Sans qu'une définition n'en soit donnée, on comprend qu'elles sont nombreuses, vont davantage dans le détail (…). Enfin (…) on peut trouver référence à des **directives**, des **mesures** ou tout simplement sur l'obligation générique de documenter ».* [441]

[37] Les politiques, procédures et mesures, s'adressent donc à des publics diversifiés au sein d'une organisation : les politiques aux directions, les

[440] article 2.60 ISO/IEC 27000:2016 (E).

[441] Vincent GAUTRAIS, *La preuve technologique*, 2ième édition, LexisNexis Canada, Montréal, 2018, p. 171 et 172, par. 223.

mesures aux opérationnels sur le terrain. Sous couvert de l'aide qu'elles proposent, les politiques, procédures et mesures ne s'auto-définissent pas et finalement ne font que mimer la hiérarchie documentaire d'origine législative en place dans une organisation. Et, de ce fait, engendrent l'inflation plus que ne participent à sa réduction.

> *« (…) cette diversité à outrance a parfois été expliqué par le fait que nous sommes face à une véritable "industrie des normes" (VERMEYS, 2010). Ces normes de l'industrie se multiplieraient donc à cause des argents quelles généreraient auprès des communautés qui les élaborent ou certifient leur application (DAUDIGEOS, 2010) »*[442]

[38] Le retour cacophonique…au droit positif. Il arrive que les normes de la famille des ISO/CEI 27 000 opèrent des renvois au droit positif: traités internationaux et législations nationales. Le renvoi s'en tient à certes à la simple interpellation quant à l'existence du droit positif, mais l'on peut aisément comprendre l'incompréhension voire l'état d'incrédulité de l'organisation qui après avoir fait la démarche de lire la loi, d'avoir accepté de se plier au jeu du renvoi à la norme, de l'avoir payée (puisqu'elle n'est pas gratuite) soit déconcertée d'en revenir au droit positif. Dans une telle situation circulaire, où est l'efficacité de la loi et où est celle des normes techniques ?

[39] Les normes mises à jour. Les normes ISO font l'objet de mises à jour. En soi, l'actualisation n'est pas critiquable – bien au contraire – puisqu'elle permet aux organismes d'être certains de l'exactitude des alertes et propositions documentaires qui leur sont faites. La cacophonie est latente à la mise à jour dans la mesure où rien n'indique aux organismes qui suivent les mises à jour s'ils doivent conserver la documentation devenue obsolète au surplus de la nouvelle documentation ou procéder à une révision complète, par la mise aux rebus, de la documentation existante. Cacophonie de l'obsolescence documentaire, cacophonie de la normativité.

[40] La cacophonie du label. Les normes de la famille ISO/CEI 27 000 apparaissent comme un label de qualité. En soi, brandir le standard ISO revient à prouver, à ceux qui le réclament, législateurs auditionnant et citoyens mécontents, que les comportements de l'organisation étaient

[442] Vincent GAUTRAIS et Pierre TRUDEL, « Mondialisation et Internet au Québec », dans Travaux de l'Association Henri Capitant des amis de la culture juridique française, La mondialisation, Journées allemandes, Bruylant et LB2V, 2016, à la page 910.

conformes au « raisonnablement attendu ». Comme la norme ISO s'accompagne de procédures d'audit, brandir le standard ISO revient à déclarer que des enquêtes de conformité à ce « raisonnablement attendu » ont été non seulement réalisées mais au surplus approuvées. Oui mais, voilà, les normes ISO ont un cout. Oui mais voilà, l'audit est une pratique récente, c'est-à-dire jeune et sans maturité. Oui, mais voilà, l'audit a aussi un cout. Et *quid* de la date de péremption de l'audit ? Quelle doit-être le laps de temps idéal entre deux audits ?

2.1.2. CACOPHONIE NORMATIVE ANNONCÉE AU REGARD DU RGPD

[41] Le RGPD… cacophonique ? Le RGPD, en tant que règlement européen, devrait avoir l'avantage de la nature et du régime juridiques des règlements européens, soit l'avantage d'une applicabilité directe, sans besoin d'une transposition de la part des législateurs nationaux[443]… Toutefois, à titre exceptionnel, le législateur européen a ouvert, avec le RGPD, une cinquantaine de brèches dans ce principe d'applicabilité directe, en autorisant les législateurs des États membres à légiférer[444].

> *« Lorsque le présent règlement dispose que le droit d'un État membre peut apporter des précisions ou des limitations aux règles qu'il prévoir, les État membres peuvent intégrer des éléments du présent règlement dans leur droit dans la mesure nécessaire pour garantir la cohérence et pour rendre les dispositions nationales compréhensibles pour les personnes auxquelles elles s'appliquent »[445].*

[42] Cette latitude du législateur européen permet au législateur de chaque État membre de : « introduire des dispositions nationales »[446], « introduire des dispositions plus spécifiques »[447], « introduire des conditions supplémentaires, y compris des limitations »[448]. Ces brèches pourraient donc favoriser l'inflation législative au sein des États-membres.

[443] Traité sur le fonctionnement de l'Union européenne (C326/49), article 288 alinéa 2.

[444] saisine 2018-765 DC du Conseil constitutionnel reçue au greffe le 16 mai 2018 (à la page 1) http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/cc2018765dc_saisine.pdf; voir également Matthieu Bourgeois et Marion Moine, La nouvelle loi informatique et libertés, une transposition du RGPD? La semaine juridique Entreprise et Affaires, numéro 30 du 26 juillet 2018, 1417 « De manière inhabituelle pour un règlement communautaire, le RGPD aménage la faculté, pour les États-membres, de transposer dans leur droit national, certaines dispositions, qui, à défaut, n'auront pas d'applicabilité directe dans leur ordre juridique interne ».

[445] Règlement (UE) 2016/679, considérant 8.

[446] Règlement (UE) 2016/679, considérant 10.

[447] Règlement (UE) 2016/679, considérant 19.

[448] Règlement (UE) 2016/679, considérant 53.

La France a utilisé ces brèches pour légiférer et modifier, *in fine*, la loi dite Informatique et Libertés[449]. Si le législateur européen offre une possibilité de légiférer, reste qu'il n'ira probablement pas vérifier le nombre de textes finalement adoptés par le législateur de chaque État-membre. Il n'ira donc pas vérifier les disparités juridiques entre États membres qu'il aura engendrées. Les règlements communautaires, d'ordinaire si strictes[450], ont opéré un virage en matière de souplesse ! Cette inflation législative qui guette chaque État membre laissé à lui-même face aux brèches et aux oublis du législateur, génèrera, par ricochet, une inflation documentaire…

[43] Le RGPD et la cacophonie documentaire. Un second phénomène se dégage, en marge des brèches que nous venons d'évoquer. Ce phénomène est semblable au cas canadien, avec la valse des « *mesures* », lesquelles sont pléthore[451], et de quelques « *politiques* » (évoquées à pas moins de 63 reprises) qui jalonnent ponctuellement le RGPD et sont une porte ouverte à la normativité alternative. Citons, par exemple,

> *« Lorsque cela est proportionné au regard des activités de traitement, les mesures visées au paragraphe 1 comprennent la mise en œuvre de politiques appropriées en matière de protection des données par le responsable du traitement »*[452]

> *« Les États membres, les autorités de contrôle, le comité et la Commission encouragent l'élaboration de codes de conduite destinés à contribuer à la bonne application du présent règlement, compte tenu de la spécificité des différents secteurs de traitement et des besoins spécifiques des micro, petites et moyennes entreprises »*[453].

[44] En France, cette cacophonie documentaire a gagné la Commission Nationale de l'Informatique et des Libertés, autrement connu sous l'acronyme CNIL. Ainsi la CNIL, dont le rôle a notamment été d'accompagner les organismes concernés par le RGPD dans leur transition a t-elle précisé, dans l'une des fiches d'accompagnement qu'elle a produite, que :

[449] Loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles (JORF n°0141 du 21 juin 2018).

[450] Traité sur le fonctionnement de l'Union européenne (C326/49), article 288 alinéa 2.

[451] « mesures raisonnables », « mesures spécifiques », « mesures appropriées et spécifiques », « mesures techniques », « mesures techniques et organisationnelles », « mesures de sécurité », « mesures correctrices », « mesures visant à produire des effets juridiques », « mesures visant à infliger des amendes administratives ».

[452] Règlement (UE) 2016/679, article 24 alinéa 2.

[453] Règlement (UE) 2016/679, article 40 alinéa 1.

« pour prouver votre conformité au (RGPD), vous devez constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu »[454].

La CNIL poursuit en indiquant ceci :

« Votre dossier devra notamment comporter les éléments suivants: la documentation sur vos traitements de données personnelles – le registre des traitements, les analyses d'impact relatives à la protection des données –, l'information des personnes – les mentions d'information, les modèles de recueil du consentement des personnes concernées, les procédures mises en place pour l'exercice des droits-les contrats qui définissent les rôles et les responsabilités des acteurs-les contrats avec les sous-traitants, les procédures internes en cas de violation des données, les preuves que les personnes concernées ont donné leur consentement lorsque le traitement de leurs données repose sur cette base. Vous avez franchi cette étape si votre documentation démontre que vous respectez les obligations prévues le règlement européen »[455].

[45] Cette fiche s'intitulant « documenter la conformité » délivre un message clair : il importe que les organismes… documentent. Si la CNIL a été prolixe sur l'énumération des types de documentation, elle n'a pas dit concrètement ce qu'il fallait faire. Une autre fiche de la CNIL, la fiche 5, se présente de la même manière. En effet, se dénommant « Organiser les processus internes », elle propose la mise en place de « procédures internes », « un plan de formation et de communication »[456].

[46] La cacophonie documentaire, dénoncée par les destinataires du RGPD. De façon bien involontaire, l'effet de « mode » autour du RGPD a été la source d'arnaques, reposant notamment sur une prestation d'aide à la documentation[457] (en marge de la prolifération des logiciels de *ransom hack* qui permettent aux pirates d'infiltrer un ordinateur et d'exiger une rançon pour éviter une fuite de données, laquelle engendrerait une amende qui pourrait, avec le RGPD, monter jusqu'à 4% du chiffre

---

[454] Commission Nationale de l'Informatique et des Libertés, https://www.cnil.fr/fr/documenter-la-conformite, 28 juin 2018 (consulté le 26 juillet 2018).

[455] https://www.cnil.fr/fr/documenter-la-conformite CNIL, 28 juin 2018 (consulté le 26 juillet 2018).

[456] étape 5 de la CNIL, organiser les processus internes 2 mars 2017 (consulté le 26 juillet 2018) https://www.cnil.fr/fr/organiser-les-processus-internes

[457] voir en ce sens les alertes de la CNIL, Pratiques abusives "Mise en conformité RGPD": comment s'en prémunir avec la CNIL et la DGCCRF, 13 juin 2018 https://www.cnil.fr/fr/pratiques-abusives-mise-en-conformite-RGPD-CNIL-DGCCRF(consulté le 1er aout 2018), voir également, DGCCRF, Pratiques abusives "Mise ne conformité RGPD": comment s'en prémunir?, 14 juin 2018 https://www.economie.gouv.fr/dgccrf/pratiques-abusives-mise-en-conformite-rgpd-comment-sen-premunir (consulté le 1er aout 2018).

d'affaires annuel mondial). S'il y a eu des arnaques, c'est peut-être bien en raison de cette cacophonie. Les principaux destinataires du RGPD ont très vite dénoncé le manque de clarté et d'accessibilité du RGPD en terme d'obligations, pointant même, pour certains, une défaillance de la CNIL dans sa mission de soutien.

2.2. ÉTAT DE L'ÉNORME DANS LA NORME : L'ADOLESCENCE DOCUMENTAIRE

[47] Constat. Le besoin de diligence est en hausse et s'intensifie à mesure que les scandales se multiplient et que les actes de délinquance immatérielle se répètent. La cadence s'est accélérée entre 2017 et 2018, avec la survenance, à quelques mois d'intervalle, de plusieurs évènements d'envergure, affectant des organismes de la scène internationale. Réseaux sociaux, compagnies aériennes, plateformes de transport de personnes, etc. ont été la cible d'attaques ou au cœur de traitements non licites et non transparents des données dont ils avaient la garde. Si les organismes doivent prouver la diligence de leur comportement, au cours d'auditions parlementaires ou à l'occasion de procès, ils doivent aussi convaincre leurs utilisateurs, dans le cas des réseaux sociaux, et leurs clients, dans le cas de sociétés commerciales de leur fiabilité. Au-delà des liens contractuels qui les lient à leurs clients ou utilisateurs, les organismes doivent aussi prouver leur diligence, de manière plus large, à « tous » : Une responsabilité accrue se vérifie donc tant au plan contractuel qu'en ce qui a trait à une responsabilité plus symbolique, morale, pour rassurer et assurer la réputation et la fiabilité de l'organisme sur la place publique médiatique.

[48] La documentation dans sa période adolescente. La diligence se prouve par la production de documents. Si plusieurs lois citées dans la première partie de notre article sont anciennes, restent qu'elles sont lacunaires en matière de documents. Les normes, auxquelles elles délèguent sont récentes et parfois tout aussi lacunaires[458]. La documentation est dans sa période adolescente : une période

[458] Voir sur ce point, V. GAUTRAIS, « Révolution numérique et quête de davantage de garanties normatives : les algorithmes sous contrôle » dans C. THIBIERGE, *précité*, note 35, à paraitre. Vincent Gautrais écrit, à ce sujet que : « (…) il est étonnant de constater parfois une vacuité et d'en d'autres cas, une substance très voire trop générale en terme d'obligations. Les normes techniques pêchent donc (par) le « pas assez » (…) ».

d'incertitude qui se traduit par une « substance trop peu engageante »[459] et des juges qui conçoivent mal la manière de les interpréter[460]. Il est probable que ces normes gagneront en maturité dans les années à venir : elles seront alors d'une grande utilité. Mais pour le moment, ces lacunes se traduisent minimalement à deux niveaux. D'abord, il est difficile pour les usagers de savoir à quelle norme se vouer et comment traduire ces textes techniques et peu précis en documentation. Ensuite, les États ont de la difficulté à gérer l'interrelation nécessaire entre droit dur et droit mou.

2.2.1. ADOLESCENCE DOCUMENTAIRE DES USAGERS

[49] Adolescence contractuelle. Avant d'être responsables devant les commissions parlementaires qui les auditionnent et les juges lorsqu'ils sont assignés en justice, les organismes le sont vis-à-vis de leurs co-contractants, c'est-à-dire leurs clients, dans le cadre de l'exécution des prestations de service, et leurs utilisateurs dans le cas des réseaux sociaux. Leurs responsabilités sont d'abord contractuelles, avant d'être une responsabilité plus symbolique. Malheureusement, ces responsabilités reposent sur une documentation encore trop incertaine, ce qui peut expliquer l'interrogation et la perte de confiance des utilisateurs et clients. Mais de façon peut-être plus troublante c'est que le contrat est le moyen de se décharger de la propre responsabilité. Beaucoup d'avocats en droit de la vie privée le diront, avec le RGPD, toute une série de contrats a été conclu afin d'exonérer les gestionnaires de données. En effet, et afin de se conformer à la législation, il importait de faire prendre conscience soit à des sous-traitants ou à des usagers qu'ils étaient responsables ou co-responsables de l'utilisation des données. Le contrat perd donc sa fonction initiale basée sur un meilleur contrôle des données[461] ; en fait, il sert désormais à protéger l'entreprise utilisatrice.

[459] Vincent Gautrais écrit à ce sujet : « Une série de critiques peut aussi être envisagée en ce qui a trait à certaines normes techniques du fait de la seule référence à la documentation. Prenons par exemple le cas de normes de la famille ISO 27000. L'analyse de la norme ISO 27002 est particulièrement frappante dans la mesure où si celle-ci réfère à de nombreuses reprises à la notion de documentation, et ce, sous des appellations variables, il n'y a que très peu de développements quant au contenu de celles-ci. L'obligation est donc de documenter mais bien peu de choses ne viennent encadrer jusqu'où ! » Vincent GAUTRAIS, « Révolution numérique et quête de davantage de garanties normatives : les algorithmes sous contrôle » dans C. THIBIERGE, *précité*, note 35, à paraitre.

[460] Vincent GAUTRAIS, « Preuve et développement durable : objectivation du droit par la normativité individuelle », dans Vincent GAUTRAIS et Mustapha MEKKI, *Preuve et développement durable*, Montréal, Éditions Thémis, 2016, pp. 43-74.

[461] Vincent GAUTRAIS, « Contrat électronique : plus de 20 ans certes mais pas encore adulte », dans Georges Decocq, Pierre-Yves Gautier, Agathe Lepage et Jérôme Passa (Dir.), *Etudes en l'honneur du professeur Jérôme Huet*, Paris, LGDJ, 2017, 430 p.

[50] Adolescence normative. Comme nous avons pu déjà le constater, il y a trop de normes[462]. Les normes étant dépourvues de force obligatoire, chaque organisme est libre d'adhérer, dans ce supermarché, aux *corpus* de normes qu'il jugera convenir le mieux à ses activités. Chaque organisme agira selon ses propres intérêts et ses propres capacités matérielles d'importation de la norme au sein de sa structure (moyens humains et financiers). Il n'y a donc pas d'uniformisation. Un peu comme dans le marché de l'automobile au début du 20ième siècle, pour reprendre un exemple soulevé par Ethan Katsh, l'immaturité su secteur d'activité faisait en sorte qu'il n'y avait pas de standards communs pour les pièces utilisés. Face à ce constat, il était difficile de déterminer lesquelles étaient les meilleures, les plus sécuritaires. Il fallut des décennies afin que le marché se stabilise.

[51] Adolescence de l'audit ? L'audit est une enquête qui peut être diligentée par des salariés de l'organisme ou par un prestataire extérieur. Cette enquête vérifie que les conditions requises sont mises en œuvre et respectées au sein de l'organisme. L'audit a valeur de preuve et ce de façon différente selon s'il est mené à l'interne ou par un prestataire extérieur[463]. L'audit est une pratique nouvelle dans le paysage de la documentation liée aux systèmes d'information. La critique de l'adolescence resurgit. L'audit tend aussi à devenir une arme redoutable, entre les mains des institutions, comme l'a récemment démontré l'actualité, dans l'affaire Facebook-Cambridge Analytica[464].

[52] Amplification du phénomène du traitement médiatique. Les organismes doivent faire face à une autre forme de responsabilité. Cette responsabilité n'est pas de nature juridique. Elle est symbolique et s'étend au-delà de la clientèle ou du réseau d'utilisateurs. Il s'agit de la réputation. La réputation peut faire perdre une clientèle potentielle à l'organisme ou plus simplement avoir pour effet de valoriser (involontairement) la concurrence. Le seul moyen pour éviter que cela n'arrive, et parce qu'en

[462] Voir Vincent GAUTRAIS, « Révolution numérique et quête de davantage de garanties normatives : les algorithmes sous contrôle » dans C. THIBIERGE, *précité*, note 35, à paraitre. Vincent Gautrais écrit, à ce sujet « En premier lieu, les normes provenant de l'industrie sont, contrairement à l'idée souvent préconçue, relativement nombreuses » (à la page 4).

[463] Vincent GAUTRAIS, « Preuve et développement durable : objectivation du droit par la normativité individuelle », dans Vincent GAUTRAIS et Mustapha MEKKI, Preuve et développement durable, Montréal, Éditions Thémis, 2016, pp. 43-74.

[464] Voir en ce sens le communiqué de presse du Parlement européen qui annonçait, le 25 octobre 2018, que « Dans une résolution adoptée (en octobre 2018) en plénière, les députés invitent instamment Facebook à permettre aux organes de l'UE de réaliser un audit complet en vue d'évaluer la protection des données et la sécurité des informations à caractère personnel des utilisateurs (...) » http://www.europarl.europa.eu/news/fr/press-room/20181018IPR16525/facebook-cambridge-analytica-des-mesures-pour-proteger-la-vie-privee (consulté en novembre 2018).

l'absence de relation juridique entre l'organisme et sa clientèle potentielle il n'y a d'autres moyens de communication que les médias papiers ou en ligne, la documentation va prendre la forme de communiqués de presse. Cette documentation n'est pas toujours juridique[465] ni ne relève des normes techniques. Pourtant, elle permet de prouver une certaine diligence. Si ces communiqués se multiplient trop souvent, ils serviront aussi d'alerte parce qu'ils résonneront comme un aveu d'incompétence dans la surveillance et la bonne gestion des données.

2.2.2. ADOLESCENCE DOCUMENTAIRE DE L'ÉTAT

[53] Mauvaise interaction entre droit dur et droit mou. Lorsqu'un manquement est décelé, il faut prouver au pouvoir législatif ou au pouvoir judiciaire, en versant au débat les documents les plus probants. Cette obligation de prouver passe par la capacité à produire des documents qui répondent, tant sur le fond que sur la forme aux exigences de la loi. Or, nous l'avons souligné, la loi n'est pas bavarde, puisqu'elle renvoie aux normes techniques et aux standards.

[54] Sources floues. « *State is not the solution, State is the problem* »[466]. Benoit Frydman l'explique dans cet article de 2012, il y aurait :

> *« (…) des formes d'hybridation des règles juridiques avec d'autres champs normatifs : la régulation économique avec les marchés artificiels (…) les « contraintes » technologiques, notamment dans le domaine informatique des réseaux de communication et des univers virtuels ; les normes managériales, notamment dans les dispositifs d'évaluation et de gouvernance par les indicateurs ; les standards techniques, notamment par l'extension du domaine des normes ISO et plus généralement par la colonisation par les standards techniques de domaines récemment couverts par des règles juridiques classiques, notamment les domaines de la santé, de la sécurité, de l'environnement, etc. »*[467]

[465] Ceci dit, elle a été intégrée dans plusieurs lois où il existe désormais une obligation de déclaration. La Loi sur la protection des renseignements personnels et les documents électroniques (LPRDE) sanctionne le défaut de déclaration « *au Commissariat à la protection de la vie privée du Canada toute atteinte aux mesures de sécurité présentant un risque réel de préjudice grave, et d'en aviser les intéressés (article 10.1)* ». Voir le communiqué du Commissariat à la protection de la vie privée du Canada, https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/conseils-au-parlement/2018/parl_sub_180529/ et https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/atteintes-a-la-vie-privee/comment-reagir-a-une-atteinte-a-la-vie-privee-dans-votre-entreprise/gd_pb_201810/ (consulté en novembre 2018).

[466] Regan Reagan, cité par Benoit Frydman, *Comment penser le droit global ?* Working papers du Centre Perelman de philosophie du Droit, 2012/01, http://wwwphilodroit.be

[467] Benoit Frydman, *Comment penser le droit global ?* Working papers du Centre Perelman de philosophie du Droit, 2012/01.

[55] Le droit dur qui est muet, mal circonscrit voire tautologique, conduit les organisations en quête de sécurité de l'information à se tourner vers l'alternative « prêt à consommer » du droit souple. La loi délègue à des standards plus pratiques que juridiques. Les innovations vont vite. Elles sont totalement décolérées du temps législatif et trouvent de ce fait, dans les standards alternatifs, des éléments d'encadrement et de conformité à ce qui pourrait être qualifié de « *compliance* » juridique. C'est ici que le point de bascule se produit. Le silence de la loi participe à l'émergence de standards qui se transforment en normes informelles à l'apparence juridique.

[56] Sources nombreuses. Pour la professeure Catherine Thibierge, le droit souple serait des normes « *issues de « petites sources » non contraignantes du droit* »[468] édictées soit au niveau des États[469], soit à des niveaux supra-étatiques[470]. Elle rappelle qu'en France, le Conseil d'état considère le droit mou comme faisant : « *(…) partie intégrante de la normativité juridique contemporaine* »[471]. La Professeure Thibierge repère, au-delà des normes gravitant dans des sphères affiliées au pouvoir législatif, de nouvelles sources. Il s'agit de « *normes techniques* »[472], au titre desquelles, elle cite « *au niveau international, l'ISO (…) véritables normes techniques internationales* »[473]. Pour la professeure Thibierge, le droit souple connaît lui aussi une crise inflationniste[474]. Suivant la logique consistant à penser que tout phénomène d'inflation s'accompagne d'une augmentation de la documentation, il faut donc en conclure que cette inflation du droit souple se traduit par une démultiplication des supports documentaires. Si la crise inflationniste à laquelle la Professeure Thibierge fait référence s'entend au sens large, son propos est particulièrement représentatif de ce qui se passe en matière de sécurité de l'information.

[468] Catherine Thibierge, La densification normative, Dalloz 2014.834.

[469] Catherine Thibierge, *La densification normative*, Dalloz 2014.834 (Catherine Thibierge cite dans son article les « recommandations, circulaires, instructions, résolutions parlementaires et autres réponses ministérielle (…) »).

[470] Catherine Thibierge, La densification normative, Dalloz 2014.834 (Catherine Thibierge cite dans son article « (…) en droit européen, résolutions, communications, lignes directrices, avis et recommandations ».

[471] Catherine Thibierge, *La densification normative*, Dalloz 2014.834 (Catherine Thibierge cite dans son article le rapport annuel du Conseil d'État pour l'année 2013).

[472] Catherine Thibierge, La densification normative in Dalloz 2014.834.

[473] Catherine Thibierge, La densification normative in Dalloz 2014.834.

[474] Pour la professeure Catherine Thibierge : « (…) à l'évidence, la densification normative ne concerne pas que le droit, mais travaille la société tout entière, en reflet de l'explosion des sources de normes de toute nature, et non des seules sources de droit » in Catherine Thibierge, La densification normative in Dalloz 2014.834.

Les normes techniques ont proliféré dans ce domaine[475]. Elles ont explosé, comme une réponse au « trop » législatif qui n'est, en réalité, à bien y regarder, qu'un vide juridique sur le plan opérationnel, dans la vie « du tous les jours » d'une organisation. L'hyperactivité du législateur ne trouve en effet aucune traduction opérationnelle efficace pour la gestion quotidienne de la sécurité de l'information et de ses contraintes. Les questions qui se posent sur le terrain, trouvent, dans les normes de la famille des ISO 27000, des pistes de résolution : résolution pratique et résolution documentaire.

[57] Dialogue institutionnel. Cette prise de décision nous amène à nous interroger sur la manière dont le droit doit être dit et doit être reconnu. Si la communauté a un mot à dire, encore faut-il qu'il ne soit pas un discours trop lénifiant qui justifie les actions d'une industrie trop présente ; trop omniprésente. Ceci nous amène encore[476] sur la nécessité de considérer le droit « mou » non pas au regard de critères substantiels qui ont toujours été identifiés pour reconnaître l'existence d'usages commerciaux[477] mais davantage sur des critères institutionnels faisant état de la qualité de l'instance qui en est à l'origine. Ainsi, au-delà de ces critères classiques, nous croyons que, d'une part, dans une volonté de meilleure objectivation et, d'autre part, afin de remplir un objectif de fidélité descriptive, il est possible d'ajouter des critères institutionnels pour reconnaître l'existence d'usages. L'usage peut donc être reconnu en fonction de l'institution dont elle tire son origine[478].

[475] Pour des exemples, voir la norme française AFNOR NF Z 42-013, mars 2009 édictant des Spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer le conservation et l'intégralité des documents stockés dans ces systèmes.

[476] Vincent GAUTRAIS, Le contrat électronique international, Bruxelles, Bruylant, 2002, p. 220.

[477] Ainsi, on évoque souvent les critères de « fréquence », de « constance », de « répétition » pour identifier la qualité d'un usage commercial, son acceptation dans un groupe donné, et ce, comme par exemple dans une décision de la Cour d'appel du Québec (*Montréal (Ville de)* c. *Environnement routier NJR*, 2011 QCCA 1251, par. 51).

[478] Vincent GAUTRAIS, Neutralité technologique : Rédaction et interprétation des lois face aux changements technologiques, Montréal, Éditions Thémis, 2012, p. 119.