Proposition de Règlement général sur la protection des données : un regard d'ailleurs… [*]

par

Vincent Gautrais[**]

****

[*] Cet article a donné lieu à une première publication dans Nathalie Martial-Braz (dir.), *La proposition de règlement européen relatif aux données à caractère personnel*, Collection Trans Europe Experts, Société de législation comparée, Paris, 2014, pp. 464-493.

[**] Professeur titulaire, CRDP, Faculté de droit, Université de Montréal, titulaire de la Chaire en droit de la sécurité et des affaires électroniques. Courriel : vincent.gautrais@umontreal.ca. Sites: www.gautrais.com / www.lccjti.ca / www.droitdu.net. Twitter : @gautrais.

[1] La proposition de Règlement européen 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 (ci-après « Règlement 2012 »)[1] tout comme sa version amendée par le rapporteur Jan Philipp Albrecht de novembre 2013 (ci-après « Version amendée »)[2] inquiètent bon nombre d'acteurs et d'interprètes nord-américains. En fait, au-delà de la « peur », il nous semble possible de constater que ces documents volumineux (135 pages pour le Règlement de 2012 et plus de 600 pour la Version amendée) suscitent une variété d'émotions telles que l'incompréhension, l'interrogation, parfois l'opposition franche ; la satisfaction en plusieurs circonstances également. Une variété d'émotions d'autant plus grande que, d'une part, ces textes vont avoir un effet direct sur la manière de gérer les données en Amérique du Nord[3] et, d'autre part, ils nous donnent quelque peu l'impression d'être un laboratoire normatif où sont essayées plusieurs solutions dont les bases demeurent encore incertaines.

[2] L'objet du présent article est donc de proposer un regard autre, et ce, dans la continuité d'une belle rencontre ayant eu lieu en octobre 2013 à l'Université de Montréal où une confrontation avec plusieurs chercheurs européens experts sur la question[4] fit état de ces divergences de vue. Le présent document veut donc établir un survol général de certains points d'achoppement qui existent notamment dans une perspective de discussion Europe / Amérique ; zones de conflit dont il importe, dans un premier temps, d'identifier si l'on souhaite par la suite tenter de les concilier. Heureusement, de façon plus positive, ces quelques lignes nous donnerons aussi l'occasion de faire état de constats communs et de solutions communes.

[3] En fait, l'impression que nous pouvons d'ores et déjà dégager est que malgré des législations qui en bien des points se ressemblent assez, c'est bien davantage des regards plus fondamentaux qui sont susceptibles d'opposer les positions en lice. Une affaire de regard s'impose donc : nous aimerions en proposer deux ; le premier est plus extérieur, plus aérien. Le second va s'attacher davantage aux principes fondamentaux qui sous-tendent ce corpus normatif.

PARTIE 1 – Regard extérieur sur la proposition de Règlement

[1] Règlement du parlement européen et du Conseil 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 (règlement général sur la protection des données), 25 janvier 2012, 2012/0011 (COD).

[2] Jan Philipp ALBRECHT, Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), November 21, 2013. Nous ne disposons que de la seule version anglaise.

[3] L'on pense d'abord et avant tout aux articles 40 et suivants du Règlement de 2012. Mais de façon plus général, on note que le débat autour de la protection des renseignements personnels est de plus en plus discuté à l'échelle internationale.

[4] Pour plus d'information sur cette rencontre, http://www.gautrais.com/conferences/reglement-europeen-2012-et-vie-privee/.

[4] Cette première perspective entend s'interroger sur les fondamentaux autour de la protection des renseignements personnels. De façon substantielle, d'abord, il convient de dire quelques mots sur ce difficile équilibrage qui sous-tend des préalables culturels et plus généralement un questionnement sur la raison d'être des garanties offertes. Ensuite, il y a aussi lieu à développer quel que peu quant à la forme que requièrent ces deux outils législatifs.

1 – Regard général sur la protection des renseignements personnels

[5] Vittorio Villa dans un livre fréquemment cité considérait que le « bon » droit est celui qui parvenait à créer une liaison harmonieuse entre les faits et les principes théoriques qui sous-tendent un domaine en particulier[5]. Il importe selon lui de clairement identifier les « deux modèles généraux de connaissance », l'un prônant le contact avec la réalité, l'autre la mise en avant d'un préalable construit, subjectif.

[6] Or, sur ces deux registres, il y a fort à dire quant à la question de la protection des renseignements personnels. D'une part, les liens culturels qui alimentent ce domaine différent selon les pays, les populations. D'autre part, la question est neuve et il est étonnant de constater que ce débat sur le Règlement 2012 ait quelque peu occulté celui quant aux fondements de la protection des renseignements personnels.

A – Liens culturels de la protection des renseignements personnels

[7] La prédominance de la loi et notre regard de juristes tend souvent à centrer ce domaine sur le droit. Pourtant, il est étonnant de constater que la vie privée en général est très souvent une question dont la première ligne est traitée par des informaticiens, des gestionnaires, des spécialistes en sciences sociales. Nous, juristes, n'avons pas le monopole de la question. Aussi, la perspective que l'on se doit d'avoir en matière de protection des renseignements personnels est celle relative à la culture de celui qui cherche à définir la vie privée. Une culture qui va d'abord être différente selon l'appartenance géographique de celui qui analyse la notion[6]. Le meilleur exemple à cet égard est le débat juridico-médiatique qui eu lieu en 2008 autour du site français note2be où le droit a eu raison de la plateforme aujourd'hui quasiment disparue. En France, un étonnant consensus semblait de mise quand à l'illégalité de l'outil offert, le nom des professeurs associés à un établissement étant considérés comme des renseignements personnels. En effet, le TGI, la Cour d'appel de Paris, la CNIL, les ministres, les syndicats, tous, d'une même voie condamnèrent l'initiative interactive. Même la doctrine semblait assez majoritaire quant à l'obligation de « mater » l'initiative marchande[7]. La donne est pourtant fort différente dans la culture nord-américaine : de tels sites pullulent sans que l'on ne s'interroge véritablement sur leur légalité, tant leur tolérance semble de mise. Au-delà des glissements pathologiques (comme la

---

[5] Vittorio VILLA, « La science juridique entre descriptivisme et constructivisme », dans Paul Amselek, *Théorie du droit et science*, Paris, P.U.F., 1994, p. 288.

[6] *The Gazette* c. *Valiquette*, 1996 QCCA 6064 : « En fait, la vie privée représente une « constellation de valeurs concordantes et opposées de droits solidaires et antagonistes, d'intérêts communs et contraires » évoluant avec le temps et variant d'un milieu culturel à un autre. »

[7] Vincent GAUTRAIS, « Give me Five ? Traitement jurisprudentiel du commerce électronique », (2009) 21-2 *Cahiers de propriété intellectuelle* 389, note 35, disponible à < http://www.gautrais.com/publications/give-me-five-traitement-jurisprudentiel-du-commerce-electronique/ >.

diffamation), l'utilisation non consentie de certaines données semble envisageable[8] ; du moins tolérée. Cette place à la culture est d'autant plus importante que les lois respectives, notamment sur la définition de renseignement personnel, sont presque identiques. En dépit de cette identité définitionnelle, la donne culturelle est foncièrement distincte.

[8] Une vision culturelle d'autant plus prégnante dans la jurisprudence canadienne que la Cour suprême a répété à de multiples reprises que l'interprétation qui devait être faite en la matière devait intégrer cette pluralité de valeurs ; sur la base d'une vision contextuelle[9], ce difficile travail d'équilibrage entend ne pas faire l'économie de telles valeurs. Non seulement elles sont distinctes, mais il importe d'en tenir compte.

B – Bases théoriques incertaines

[9] Le droit à la protection des renseignements personnels est un droit neuf et ses bases théoriques sont pour le moins fragiles. Nous aimerions faire état de deux considérations, pourtant centrales, qui ne font pas l'unanimité.

i) Droits en concurrence

[10] En premier lieu, il importe de s'interroger sur la quête d'équilibre qui existe selon nous de façon inhérente en protection des renseignements personnels. En effet, si la protection catégorielle de l'individu est évidemment déterminante, elle doit s'analyser en tenant compte d'intérêts concurrents. D'une part, cette concurrence se matérialise au sein même de la protection des renseignements personnels où dès le départ on a voulu offrir des garanties pour compenser l'utilisation des données personnelles. C'est donc en constatant la nécessité de les faire circuler que des garanties sont apparues dans les lois. François Rigaux évoquait même le fait que la circulation est la raison pour laquelle les lois ont été adoptées, et notamment la directive européenne de 1995[10]. Cette compréhension est identique dans la Loi fédérale canadienne[11]. Or,

---

[8] *Infra*, Partie 2, Paragraphe 1, A, le débat sur la question de la définition des renseignements personnels.

[9] Sur l'approche contextuelle en matière de protection des renseignements personnels, Vincent GAUTRAIS, *La neutralité technologique : rédaction et interprétation des lois face aux technologies*, Montréal, Éditions Thémis, 2012, p. 255.

[10] François RIGAUX, « Libre circulation des données et protection de la vie privée dans l'espace européen », dans Pierre TABATONI, *La protection de la vie privée dans la société d'information*, tome 2, 2000, Presses universitaires de France, 2000, disponible en ligne à < http://www.asmp.fr/travaux/gpw/internetvieprivee/rapport2/chapitr8.pdf > : La nécessité de tenir en équilibre **deux intérêts divergents**, sans qu'aucun ne puisse, en principe, être sacrifié à l'autre, apparaît dans l'intitulé de la directive 95/46/CE du Parlement et Conseil des Communautés européennes 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. » (Nos soulignements)

[11] dans la *Loi fédérale sur la protection des renseignements personnels et les documents électroniques* (plus connue sous l'acronyme PIPEDA), L.C. 2000, c. 5, disponible à http://www.canlii.ca/ca/loi/p-8.6/, où à l'article 3, on peut lire ceci : « 3. La présente partie a pour objet de fixer, dans une ère où la technologie facilite de plus en plus la circulation et l'échange de renseignements, des règles régissant la collecte, l'utilisation et la communication de renseignements personnels d'une manière qui tient compte du droit des individus à la vie privée à l'égard des renseignements personnels qui les concernent et du besoin des organisations de recueillir, d'utiliser ou de

ce besoin de circulation est encore plus présent aujourd'hui qu'au moment où ces principes ont été identifiés. D'un côté, cette circulation accrue permet de justifier un renforcement des mesures de protection ; de l'autre, et comme mentionné plus tôt, il y a sans doute lieu d'opérer une graduation des hypothèses où un danger véritable existe.

[11] D'autre part, cette concurrence se matérialise avec d'autres corpus législatifs basés sur la défense d'intérêts catégoriels distincts. Ce questionnement préalable ne doit pas s'opérer en autarcie, la protection des renseignements personnels n'étant pas un droit autonome[12]. Par exemple, la vie privée ne peut être envisagée isolément sans que l'on considère l'impact de la défense de cet intérêt catégoriel envers d'autres droits. Aussi, elle ne peut s'accroître sans avoir une incidence sur plusieurs autres libertés fondamentales, voire certaines préoccupations étatiques, comme la sécurité nationale, dont il n'est aucunement question dans le présent règlement[13]. Les nouvelles technologies ont en effet amené à reconsidérer certains domaines du droit. Plusieurs d'entre eux ont vu leur importance s'affirmer ; à bien des égards, leur expansion se trouve limitée à celle des autres. Certains se rappelleront que, dans nos anciens cours de sciences physiques au collège, une expérience consistait à mettre un ou plusieurs ballons de baudruche sous une cloche à vide. Plus la cloche se vidait de son air, plus les ballons gonflaient, présentant ainsi des points de contact de plus en plus nombreux. Eh bien, sur Internet, le même phénomène se présente : droit d'auteur, droit à la vie privée, droit de la consommation, pour ne citer qu'eux, sont autant de droits dédiés à une cause qui prennent de l'expansion et voient leurs prérogatives réduites par les prétentions des autres droits concurrents. Internet est la cause d'une confrontation qu'il n'était pas nécessaire de prévoir dans le monde analogique tant les occurrences de contact étaient dérisoires. Désormais, on ne peut plus faire l'économie de ces débats. C'est d'ailleurs la raison pour laquelle tout récemment la Cour suprême demanda au législateur d'intervenir dans un litige en droit du travail où les parties avaient filmé des personnes traversant des lignes de piquetage[14]. En effet, dans cet équilibre entre protection de l'individu et liberté d'expression, les juges ont considéré que la délimitation devait être précisée par la loi[15].

---

communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances. »

[12] Dominique CARDON, *La démocratie Internet : Promesses et limites*, Coll. « La république des idées », Seuil, 2010, p. 44 : « Celui qui parle doit être protégé par le droit à la liberté d'expression ; celui dont on parle, par le droit à la vie privée. Comme il a été souvent souligné, il est vain de chercher à autonomiser le droit à la privacy ».

[13] Au-delà du volumineux règlement que nous évoquons ici, rien n'est en effet envisagé quant à la compatibilité avec la Directive de 2006 sur la conservation des données (*Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE*).

[14] *Alberta (Information and Privacy Commissioner*) c. *Travailleurs et travailleuses unis de l'alimentation et du commerce, section locale 401*, 2013 CSC 62.

[15] *Alberta (Information and Privacy Commissioner*) c. *Travailleurs et travailleuses unis de l'alimentation et du commerce, section locale 401*, 2013 CSC 62. « La question principale est celle de savoir si la PIPA atteint un équilibre acceptable sur le plan constitutionnel entre, d'une part, le droit des personnes d'exercer un droit de regard sur la collecte, l'utilisation et la communication des renseignements personnels les concernant et, d'autre part, la liberté d'expression d'un syndicat. »

[12] Une autre illustration peut être trouvé dans les dispositions du Règlement 2012 relatives au droit à l'oubli[16], et ce, même si la notion fut pour le moins édulcorée dans les Amendements Albrecht[17]. Au-delà du jugement de valeurs sur lequel nous ne souhaitons pas nous prononcer quant à la prévalence d'un des droits par rapport à l'autre[18] – vie privée *versus* liberté d'expression – on ne peut que constater le changement de donne que présente la balance inhérente à cet équilibre fort contextuel et que la jurisprudence dégagea peu à peu. D'abord, la nuisance qu'est susceptible d'avoir l'information exposée avec les nouveaux médias peut en certains cas être passablement destructrice. De plus en plus, Internet et autres technologies autorisent une persistance et un accès à grande échelle. Ensuite, la liberté d'expression mérite d'être évaluée en fonction du contenu du propos, de la façon dont il est dispensé ; il y a liberté d'expression et liberté d'expression, surtout quant le propos en cause est tenu anonymement[19] ; surtout lorsque l'on considère les coûts parfois associés aux efforts pour retrouver les auteurs des propos anonymes[20].

ii) Renseignement personnel et contrôle

[13] En second lieu, un débat fondamental doit s'opérer quant aux valeurs sous-jacentes à la protection des renseignements personnels. En droit américain par exemple, ce droit essentiellement jurisprudentiel a fait l'objet de vagues, successives, introduisant une valeur de plus en plus englobante[21]. Plus récemment, c'est bien la notion de contrôle des données qui fut généralement associée à la protection des renseignements personnels. Ainsi, chaque individu devrait être en mesure d'avoir un certain contrôle sur les données le caractérisant. D'ailleurs, le terme fut abondamment instrumentalisée par les *Facebook*, *Google* de ce monde qui trouvaient avec cette sous-notion un moyen d'utiliser les données tant que ce contrôle était autorisé par les individus. Si la notion fut régulièrement utilisée par les tribunaux, et notamment la Cour suprême

---

[16] Voir les articles 17 et suivants.

[17] Il semble en effet que droit à l'oubli ait été « oublié », laissant seulement à l'article 17 la protection que constitue le droit à l'effacement.

[18] Faute de temps pour développer plus avant cette notion, nous nous limiterons à témoigner d'un certain malaise avec ces notions de droit à l'oubli et de droit à l'effacement. Substantiellement, notre impression est que les atteintes à la vie privée sont davantage susceptibles de se produire dans l'ombre que dans la lumière. Plus exactement, c'est plutôt les erreurs de traitement, souvent connues par hasard, qui méritent d'être contrôlées. Pratiquement, la mise en application de ces dispositions est tout sauf aisée. Ces dispositions présentent en effet une pluralité de composantes subjectives qui risquent d'être difficiles à départager.

[19] *Prud'homme c. Rawdon (Municipalité de*), 2010 QCCA 58, par. 53 : « (...) les insultes et les injures apparaissaient gratuites et prononcées pour la plupart sous le couvert de l'anonymat. Par ailleurs, d'aucuns pourraient s'interroger sur l'étendue de la protection qui doit être accordée à la liberté d'expression lorsque de pures insultes sont proférées de façon anonyme. Ce ne sont pas toutes les expressions qui justifient une même protection »

[20] Dans l'affaire précitée, des centaines de milliers de dollars ont été dépensés afin de retracer les auteurs anonymes derrière un site dont la finalité première était de critiquer le travail d'un mairesse.

[21] Éloïse GRATTON, *Understanding Personal Information : Managing Privacy Risks*, LexisNexis, Markham (On.), 2013, pp. 2-6. Dans cet ouvrage on peut notamment constater que la première vague remonte à la fin du 19ième siècle avec « The right to be alone ». Plus tard, après la seconde guerre mondiale, est apparu[] e « The right to respect for private ans family life ». Dans les années 1960, la notion de contrôle fut communément utilisée pour identifier une troisième vague.

du Canada[22], sa généralisation fut néanmoins la source à de nombreuses critiques, notamment dans les environnements les plus récents où cet objectif est devenu en bien des cas un leurre[23].

La protection des renseignements personnels ne peut donc en toutes circonstances être associée à des données que l'individu peut contrôler ; parfois, la vie privée est extérieure à sa capacité de vouloir et doit être davantage associée à une liberté fondamentale[24]. Il n'y aurait donc pas d'opposition entre l'acception selon laquelle la protection des renseignements personnels est le moyen pour l'individu d'exercer un contrôle sur ses propres données et celle où elle est davantage un principe fondamental. Davantage, l'équilibre entre les deux notions dépend des circonstances. En effet, plus la capacité de contrôle est grande, plus les revendications en termes de dignité du citoyen seront ardues à réclamer. Inversement, moins l'individu aura une préhension sur ses propres renseignements individuels, et plus il sera en mesure d'évoquer cette dignité si recherchée. Ceci dit, et comme le verrons plus tard, cet axiome n'est pas sans exception et il est sans doute des domaines où le contrôle abandonné puisse être revisité, sur la base d'une pression indue, d'une liberté de choix trop factice.

[14] Dans cette question d'équilibrage de droits catégoriels en opposition, le juge, et notamment les juges de la Cour suprême ont souvent tenté de trouver des critères de partage. Les décisions en matière de réseaux sociaux ne manquent pas, au Canada, d'illustrer cette quête d'équilibre avec trois situations factuelles différentes. La première hypothèse est celle où l'individu s'abandonne et « sacrifie » le contrôle de ses données sur l'autel de la sociabilité[25]. En pareille hypothèse, les juges ont assez unanimement sanctionné l'intéressé pour son manque de pudeur, de bon sens parfois, conformément à l'adage latin « nul ne peut invoquer sa propre turpitude ». Au même titre que dans l'hypothèse d'une poubelle abandonnée traitée par la Cour suprême du

---

[22] *R.* c. *Patrick*, 2009 CSC 17 ; *Alberta (Information and Privacy Commissioner*) c. *Travailleurs et travailleuses unis de l'alimentation et du commerce, section locale 401*, 2013 CSC 62, par. 1: « il s'agit de savoir si la *Loi* atteint un équilibre acceptable sur le plan constitutionnel entre, d'une part, le droit des personnes d'exercer un droit de regard sur la collecte, l'utilisation et la communication des renseignements personnels les concernant et, d'autre part, la liberté d'expression d'un syndicat. »

[23] Danah BOYD, Networked Privacy. Surveillance & Society 10(3/4): 348-350, disponible à < http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/networked/networked > : « Any model of privacy that focuses on the control of information will fail. Even achieving true control is nearly impossible because control presumes many things that are often untenable. Control assumes that people have agency, or the power to assert control within a particular situation. Control assumes that people have the knowledge and skills to truly control information. And control assumes that people understand the situation well enough to make informed decisions about what should be shared to whom and when. Furthermore, in a networked age, a reasonable amount of control is not enough; control has to be absolute control. »

[24] Avner LEVIN et Patricia SANCHEZ ABRIL, « Two Notions of Privacy Online », (2009) 11 Vanderbilt Journal of Entertainment & Technology Law 1001, 1005. Lire notamment les références disponibles à la note 4 de cet article. « One theoretical assumption formulated as a possible response to the questions above, and underlying this research project, is the existence of two prevalent and competing formulations of privacy : one rooted in control and the other in dignity »

[25] Voir par exemple Brisindi c. STM (Réseau des autobus), 2010 QCCLP 4158 ; Bagasbas v. Atwal, 2009 BCSC 512 ; Bar Le « I » (Re), 2010 CanLII 8200 (QC R.A.C.J.) ; Bar Chez Le Blanc (Re), 2010 CanLII 4569 (QC R.A.C.J.) ; Dussault (Re), 2009 CanLII 73828 (QC R.A.C.J.).

Canada[26], on ne peut que moindrement protéger la vie privée d'une personne qui ne la protège pas elle-même. Le deuxième cas est celui où nos renseignements sont sous un contrôle modéré ; entendons par là que certaines informations nous concernant sont publiées, mais dans une communauté d'« amis » que nous avons nous-mêmes délimitée. Cela peut aussi correspondre à l'hypothèse où un individu pirate un réseau afin d'obtenir des renseignements qui lui sont utiles. Cette hypothèse fut avérée dans certains cas[27] ; dans d'autres, on peut s'interroger sur la capacité d'un avocat d'une partie qui affirme avoir accédé par « hasard » à certaines informations incriminantes[28]. Enfin, en troisième lieu, il y a l'hypothèse où le renseignement personnel d'un individu est tout simplement mis en ligne par autrui. Dans ce cas, bien évidemment, il n'y a aucune capacité de contrôle a priori par l'intéressé. Bien que l'hypothèse soit très différente, c'est un peu comme dans l'hypothèse où lors d'une descente de police dans une école, des chiens renifleurs décelèrent des stupéfiants dans le sac d'un des étudiants[29]. Bien que l'analyse contextuelle a évidemment été prise en compte, on peut imaginer que la notion de dignité a joué un rôle déterminant en l'espèce. Or, dans les trois hypothèses, et en ce qui a trait aux décisions liées aux nouvelles technologies, et précisément au Web 2.0, il est pour le moins étonnant de constater en droit canadien une admission sinon systématique mais pour le moins fréquente des preuves ainsi octroyées. Si cela peut se comprendre dans la première hypothèse, eu égard au contrôle possible, et non exercé par l'intéressé, c'est passablement plus problématique dans les deux autres hypothèses. Pour le moins, en Ontario, plusieurs jurisprudences amènent les juges à s'interroger sur l'admissibilité des preuves, ceux-ci les autorisant en certains cas et les refusant dans d'autres[30]. Au Québec, il est étonnant de constater que la question ne se pose souvent même pas[31].

---

[26] *R.* c. *Patrick*, 2009 CSC 17, par. 62.

[27] Droit de la famille – 09349, 2009 QCCS 665 ; 9116-8609 Québec inc. c. Senécal, 2010 QCCS 3308. On peut notamment lire dans cette dernière affaire le paragraphe 40 : « L'affi davit de Bortugno stipule, en outre, qu'il a été capable d'avoir accès à ces mêmes courriels car, après quelques essais, il a pu déterminer le nouveau mot de passe de Senécal et accéder à sa boîte de courriels. Apparemment, l'exercice fut relativement facile puisque Senécal avait l'habitude d'utiliser le nom de l'un de ses chiens ou du chien de l'un de ses proches. »

[28] Kourtesis v. Joris, 2007 CanLII 39367 (Ont. S.C.).

[29] R. c. Kang-Brown, [2008] 1 R.C.S. 45.

[30] Leduc v. Roman, 2009 CanLII 6838 (Ont. S.C.) ; Schuster c. Royal & Sun Alliance Insurance Company of Canada, 2009 CanLII 58971 (Ont. S.C.).

[31] Plusieurs décisions ne se sont même pas interrogées sur la façon dont certaines pages *Facebook* ont été obtenues. Voir notamment Renaud et Ali Excavation, 2009 QCCLP 4133 ; Garderie Les « Chat » ouilleux inc. et Marchese, 2009 QCCLP 7139 ; Pawlus c. Hum, 2008 QCCQ 11136. Pourtant, et eu égard à la difficulté d'utiliser la méthode d'interprétation fonctionnelle, téléologique, il est possible de s'inspirer des faits d'une affaire qui a finalement été traitée devant la Cour d'appel du Québec *Syndicat des travailleurs (euses) de Bridgestone Firestone de Joliette (CSN)* c. *Trudeau* (1999 CanLII 13295 (QC C.A.)). En l'espèce, il s'agissait d'évaluer l'admissibilité de vidéos qui avaient été commandées à un professionnel afin de surveiller un employé en congé de maladie qui prétendait ne pas pouvoir reprendre le travail. La Cour d'appel admit les preuves vidéos sur la base de trois conditions cumulatives qui furent en l'occurrence satisfaites. En premier lieu, cette preuve a été considérée comme nécessaire, aucun autre moyen ne pouvant être utilisé. En deuxième lieu, il y avait des motifs raisonnables de croire que l'employé feignait d'être malade et notamment la présence de rapports médicaux contradictoires. En troisième lieu, les modalités de surveillance furent jugées comme étant raisonnables et documentées, des limites furent établies avant même la confection desdites vidéos.

2 – Regards sur l'outil réglementaire

[15] Au-delà de la substance juridique, de façon plus procédurale, il nous apparaît possible d'apporter aussi un regard critique sur le règlement en tant qu'outil législatif. Nous aimerions identifier ici, là-encore, deux directions. La première entend traiter de la pertinence de la voie législative choisie forcément par ce règlement. La seconde est plus liée à la forme législative à proprement parler.

A – Choix normatif

[16] En Amérique du Nord, le reflexe législatif est sans doute moins systématique qu'en Europe. Culturellement encore, l'intervention formelle de la loi est davantage vu comme un dérangement qui intervient lorsqu'une situation pathologique est consacrée. À titre d'illustration, et comme vu précédemment, la Cour suprême du Canada est intervenue en sommant le législateur de préciser un point de droit quant à la définition du renseignement personnel[32]. Mais plus souvent qu'autrement, la capacité de nuisance de la loi n'est pas sous-estimée, celle-ci n'étant pas forcément synonyme de progrès.

[17] Dans la lignée des propos qui avait été développés par Larry Lessig, il y a une concurrence des moyens pour insuffler une direction à un comportement que l'on juge illégitime. Le premier qui peut évidemment être utilisé pour ce faire est le « Droit ». Bien sûr, la loi est l'outil par excellence dont le Canada dispose d'ailleurs grâce à la directive européenne de 1995 et à ses dispositions de transferts internationaux de données[33]. Notons à cet égard qu'il peut paraître étrange de voir un canadien critiquer la loi d'une juridiction étrangère eu égard aux défauts inhérents qui sont propres à la sa loi nationale[34]. En effet, actuellement celle-ci est d'une rare incapacité d'action avec des prérogatives ridiculement faibles. De façon assez ahurissante, cette organisation ne peut imposer de sanctions financières comme cela vient d'être fait contre *Google* en France. À dessein, Jennifer Stoddart, commissaire fédéral à la vie privée, réclame d'ailleurs plus de pouvoirs au Commissariat et parmi eux des pouvoirs pécuniaires de sanction. Cette quête pour plus de prérogatives aux institutions en charge de faire appliquer la loi est d'autant plus importante que la jurisprudence n'a à ce jour que très peu sanctionné des infractions suite à une poursuite personnelle des victimes[35]. Ces victimes, qu'elles soient des personnes physiques ou morales, ne sont donc que très peu motivées à ester en justice pour faire valoir leur droit.

---

[32] *Alberta (Information and Privacy Commissioner*) c. *Travailleurs et travailleuses unis de l'alimentation et du commerce, section locale 401*, 2013 CSC 62.

[33] L'article 25 de la Directive de 1995 imposa au Canada de disposer d'un régime de protection jugé adéquat. La Loi fédérale de 2000 a notamment été adoptée afin de satisfaire à cette exigence ; une exigence reconnue comme étant satisfaite selon un avis de la commission européenne en décembre 2001.

[34] Dans un communiqué rendu public en mai 2013, la Commissaire Stoddart réclame des mesures plus vigoureuses pour sanctionner les atteintes à la protection des renseignements personnels. Voir notamment le communiqué disponible à < http://www.priv.gc.ca/media/nr-c/2013/nr-c_130523_f.asp >.

[35] Le droit à la vie privée étant une prérogative individuelle reconnue dans plusieurs textes de lois, soit spécifiques à la protection des renseignements personnels soit généraux et notamment les articles 35 et suivants du Code civil du Québec, rien n'empêche un individu d'intenter une action sur cette base. Dans les faits, bien peu d'affaires ne donnent lieu à de telles actions et a fortiori de dédommagements.

[18] Face à cet état de fait, cet état de droit devrait-on dire, plusieurs initiatives de normes informelles furent mises de l'avant. Le Commissariat en développa lui-même, tout comme d'autres commissariats provinciaux. Le droit n'est donc pas vu uniquement comme un moyen de sanction mais aussi comme un outil permettant une approche collaborative. À cet égard, Il nous importe de dire quelques mots sur la démarche employée par le Commissariat canadien en 2009 contre *Facebook*. Comme partout ailleurs, plusieurs infractions de la multinationale états-unienne furent constatées. Dans les circonstances, au Canada, l'approche judiciaire était pour le moins fantaisiste ; nous avons souligné le caractère édenté des « crocs » dont notre loi dispose et les questionnements en terme de droit international privé sont loin d'être simples à résoudre. Cette institution négocia donc avec la multinationale avec un résultat étonnant, faisant assurément plusieurs gains en terme de transparence et aussi en ce qui a trait à la satisfaction de la loi canadienne[36]. Notons aussi que chez notre voisin du sud, le *Federal Trade Commission* (FTC) a également négocié avec *Facebook*, ce dernier consentant à « ouvrir ses livres », certains audits devant être fait par l'organisation gouvernementale américaine durant les 20 prochaines années[37]. Cette option communicationnelle, plus que juridique, ce que Larry Lessig identifie sous le terme de « normes sociales » était dans les circonstances sans doute la plus appropriée. Là encore, loin de nous l'idée de considérer cette solution comme meilleure que la voie plus rigoureusement légale. Elle traduit néanmoins une démarche qui n'est pas rare en Amérique du Nord, et ce, même dans les hypothèses où l'enjeu est la protection du citoyen.

[19] Si besoin était, et selon cette même approche, on peut encore mentionner la toute récente négociation entre *Google* et le Commissariat canadien à la vie privée qui demeure foncièrement distincte de celle que l'on trouve en Europe[38]. Notons d'ailleurs que dans cette affaire concernant ce que l'on appelle la publicité comportementale, l'illégalité du comportement s'est basée principalement sur une norme informelle interne que le Commissariat avait élaborée quelques mois plus tôt[39]. L'informalité du processus juridique se ressent donc tant dans le traitement de la norme que pour la norme elle-même.

B – Forme législative

---

[36] Plusieurs modifications furent demandées, et obtenues, afin que les usagers *Facebook* soient mieux informés du traitement de leurs données personnelles. Malheureusement, cette meilleure information se concrétisa souvent par le simple ajout de stipulations dans le contrat liant la multinationale aux usagers. Contrat dont on peut douter de la lecture par l'utilisateur moyen. Le droit était donc respecté ; quant à une meilleure protection de ce dernier…

[37] Selon une procédure très américaine, qui prévaut dans plusieurs domaines du droit, il est possible de reconnaître judiciairement certains accords conclus entre une instance gouvernementale et une compagnie privée. Aussi, le 29 novembre 2011, Facebook accepta de s'engager à être davantage transparent dans l'utilisation des renseignements personnels de ses « membres ». Pour plus d'information, voir <http://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookagree.pdf >.

[38] On peut notamment trouver un communiqué de presse où les parties en cause semblent se féliciter des concessions mutuelles qui ont été faites. http://www.priv.gc.ca/media/nr-c/2014/nr-c_140115_f.asp.

[39] Lignes directrices concernant la protection de la vie privée et la publicité comportementale en ligne, juin 2012, disponible à < http://www.priv.gc.ca/information/guide/2011/gl_ba_1112_f.asp >.

[20] Souvent, les lois relatives aux technologies sont d'une longueur impressionnante ; fait étrange, un néologisme a été inventé, pire déifié, justement pour tenter de contrer cette pathologie législative. Il s'agit de la neutralité technologique.

i) Longueur du Règlement

[21] Vu de l'extérieur, le Règlement 2012 comme sa Version amendée peut surprendre. Au-delà de la technique des considérants (pas moins de 139 !!!), dont nous ne connaissons rien, il est étonnant de constater la longueur imposante du document qui par ce seul élément fait craindre des difficultés interprétatives. A titre de comparaison, une proposition parlementaire d'amendement de la Loi fédérale canadienne faisait en 2013 moins de 4 pages…[40] Aussi, face à ce fléau qui n'est ni l'apanage des textes en droit des technologies[41] ni propre au droit civil[42], il nous est pourtant permis de constater que cette expansion législative n'est généralement pas source à simplicité. À bien des égards, et de façon paradoxale, les anciens textes sont souvent la source de plus d'adaptation que les nouveaux[43]. Bien évidemment, les changements législatifs s'imposent souvent mais la main tremblante préconisée depuis longtemps pour rédiger des textes formels devrait ne pas être oubliée[44]. Il est vrai que le contexte continental ne facilite pas la donne : parfois, la quête d'uniformisation, que ce soit au plan international ou régional, est source à perte de cohérence. N'oublions pas non plus que ce texte substantiel n'est pas le seul qui

---

[40] Projet de loi C-475, 2013, disponible à < http://droitdu.net//fichiers/20130409_c_475.pdf >.

[41] CONSEIL D'ÉTAT, *Rapport d'activité 2006*, Paris, Documentation française, 2006, p. 265 et 266, en ligne : <http://www.ladocumentationfrancaise.fr/rapports-publics /064000245/index.shtml> (consulté le 7 février 2012) : « D'une longueur moyenne de 15 000 pages par an au cours des années 1980, le Journal officiel comporte plus de 23 000 pages annuelles au cours des dernières années. Le Recueil des lois de l'Assemblée nationale est passé de 433 pages en 1973 à 1067 pages en 1983, 1274 pages en 1993, 2400 pages en 2003 et 3721 pages en 2004. »

[42] Chris REED, « How to Make Bad Law : Lessons from Cyberspace », (2010) 73-6 *Modern Law Review* 903, 904 et 905.: « Across all fi elds of law there is a clear trend for legislation and regulation to become increasingly detailed. As an example, the UK Companies Act 1948 consisted of 462 sections and 18 Schedules, whereas the 2006 Act runs to 1,300 sections and 16 Schedules. Much of that increase is because of an attempt to spell out the law's requirements in exhaustive detail, rather than as broad obligations of principle. In 1948 the provisions relating to auditors occupied only seven sections of the Act ; in 2006 a full 65 sections were needed, perhaps ten times as much detail. »

[43] Vincent GAUTRAIS, *La neutralité technologique : rédaction et interprétation des lois face aux technologies*, Montréal, Éditions Thémis, 2012, p. 161.

[44] Charles de Secondat DE MONTESQUIEU, « Lettre CXXIX, de Usbek à Rhédi », dans Lettres Persanes, 1719, en ligne à < http://visualiseur.bnf.fr/Visualiseur?Destination=Gallica&O=NUMM-101473 > (consulté le 28 février 2014) : « Il est vrai que, par une bizarrerie qui vient plutôt de la nature que de l'esprit des hommes, il est quelquefois nécessaire de changer certaines lois. Mais le cas est rare ; et, lorsqu'il arrive, il n'y faut toucher que d'une main tremblante : on y doit observer tant de solennité, et apporter tant de précautions, que le peuple en conclu naturellement que les lois sont bien saintes, puisqu'il faut tant de formalités pour les abroger. » L'expression fut ensuite reprise par Jean CARBONNIER, « Scolie sur le non droit », dans *Flexible droit. Pour une sociologie du droit sans rigueur,* Paris, L.G.D.J., 2001, p. 50 : « [...] Ce serait déjà un beau résultat si nos hommes du gouvernement consentaient à prendre conseils de quelques maximes, inspirées de l'hypothèse et pourtant raisonnables telles Ne légiférez qu'en tremblant, ou Entre deux solutions, préférez toujours celle qui exige le moins de droit et laisse le plus aux moeurs ou à la morale. »

prévaudra en protection des renseignements personnels et qu'il devra s'ajouter à d'autres en la matière[45].

ii) Neutralité technologique

Sur le plan formel encore, nous avons été également surpris de l'instrumentalisation de la notion de neutralité technologique qui semble tant être une caractéristique respectée par le Règlement[46] qu'un objectif à satisfaire[47]. Sans être opposé à cette qualité, nous ne sommes pas persuadé ni de la réalité de cette affirmation ni de sa pertinence à tout coup.

[22] En premier lieu, nous souhaitons nous interroger sur le fait que le Règlement de 2012 soit neutre sur le plan des technologies[48]. Car que veut dire cette expression bien peu souvent précisée et utilisée dans le Règlement comme une évidence ; avec une affirmation sujette à caution[49]. Selon nous, il s'agit de la qualité d'une loi qui ne cherche pas à favoriser une technologie plutôt qu'une autre ; il s'agit donc d'une méthode législative qui tente d'être le plus en retrait possible avec les solutions existantes et ainsi transposables à celles qui n'existent pas encore. Or, ce souhait, en bien des cas, est un vœux pieux. Il nous semble important de garder en tête que les principes fondamentaux de la protection des renseignements personnels datent d'une époque où la technologie prédominante était les bases de données[50]. Ainsi, elle prenait généralement appui sur un principe que plus le contrôle des données était assuré et plus la protection était consacrée. Une meilleure protection passait donc par une immobilisation des données ; la communication à autrui devait donc pouvoir bénéficier d'une exception et notamment de celle que constitue souvent le fameux consentement. Or, le défi d'aujourd'hui est justement « de garantir la protection dans un contexte où les renseignements circulent »[51]. Ce cloisonnement initial n'est plus la norme ; il est non seulement difficile à maintenir tant la circulation devient une réalité croissante mais de surcroît cette dernière est dans bien des cas un

---

[45] On peut notamment penser aux corpus de règles qui prévalent en ce qui a trait à la Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, *Journal officiel n° L 105 du 13/04/2006 p. 0054 – 0063*.

[46] Voir par exemple les considérants 13, 66.

[47] Dans l'exposé des motifs du Règlement, la notion est vue à plusieurs reprises (par exemple page 5).

[48] Nous allons reprendre ici seulement quelques arguments que nous avons développé plus substantiellement dans un livre paru en 2012. Vincent GAUTRAIS, *La neutralité technologique : rédaction et interprétation des lois face aux technologies*, Montréal, Éditions Thémis, 2012. Ce livre est disponible en ligne sur www.gautrais.com.

[49] À titre d'illustration, nous avons de la difficulté à comprendre le considérant 13 qui évoque la dangerosité du non respect de la neutralité technologique : « La protection des personnes devrait être neutre sur le plan technologique et ne pas dépendre des techniques utilisées, sous peine de créer de graves risques de contournement. »

[50] Neil ROBINSON, Hans GRAUX, Maarten BOTTERMAN et Lorenzo VALERI, *Review of the European Data Protection Directive, RAND Europe Technical Report*, Santa Monica, RAND Corporation, 2009, en ligne : http://ico.org.uk/about_us/research/~/media/documents/library/Data_Protection/Detailed_specialist_guides/REVIEW_OF_EU_DP_DIRECTIVE_SUMMARY.ashx.

[51] Vincent GAUTRAIS et Pierre TRUDEL, *Circulation des renseignements personnels et web 2.0,* Éditions Thémis, Montréal, 2010, p. 15.

moyen d'offrir des services de meilleure qualité aux citoyens des États et aux clients des entreprises. À certains égards, on pourrait aussi prétendre que la mise de l'avant, fort intéressante, de la documentation est une nouveauté propre aux technologies actuelles[52]. Si cette notion était moins présente dans la Directive de 1995, c'est en partie à cause du fait que cette solution était sans doute moindrement adaptée aux banques de données. Nous y reviendrons.

[23] En second lieu, il est également possible de douter de la pertinence d'avoir des lois neutres[53]. D'ailleurs, dès que l'on touche aux technologies, les lois ne manquent pas de s'adresser à des cas particuliers : le droit d'auteur est l'exemple même de textes qui s'adaptèrent aux évolutions techniques au cas par cas ; la diffamation est susceptible d'être bouleversée par la capacité de nuisance, l'anonymat et la persistance de l'information ; la plupart des lois récentes sur les contrats électroniques visent d'abord et avant tout, et malgré leur neutralité technologique supposée et déclarée, à justement favoriser l'usage des technologies nouvelles. Cette neutralité face aux technologies est particulièrement difficile à satisfaire pour des domaines du droit qui souvent sont donc intimement liés à ces premières[54].

PARTIE 2 – Regard intérieur sur la proposition de Règlement

[24] Après ces considérations plus aériennes, préalables, à la proposition de Règlement, nous aimerions développer plus avant le cœur de ces deux documents ; du moins certains de leurs aspects qui nous apparaissent centraux. Là encore, et dans ce choix de sujets à traiter, deux directions peuvent être envisagées : dans un premier temps, nous souhaitons envisager certaines des solutions substantielles qui caractérisent ce texte. D'autres, plus procédurales, pourront ensuite être développées.

1 – Solutions substantielles

[25] Obligé de faire un choix, il y a deux aspects sur lesquels il nous semble utile d'apporter un point de vue extérieur. D'abord, la notion même de renseignement personnel tend à être considéré en Amérique du Nord avec moins de largesse qu'en Europe. Ensuite, le consentement sera envisagé du fait de son importance et eu égard à son utilisation pour le moins pathologique, et ce, des deux côtés de l'Atlantique.

A – Domaine d'application très large de la proposition de Règlement

[26] Le Règlement de 2012 entend disposer d'un domaine d'application très large. Ceci se vérifie tant la définition de renseignement personnel que de celle de traitement. Une volonté inclusive qui n'est d'ailleurs pas une nouveauté et qui se trouvait également dans la Directive de 1995.

---

[52] *Infra*, Partie 2, Paragraphe 2, A, s'intitulant « Documentation ».

[53] Sans prétendre exhaustive, ce courant s'intensifie. Par exemple Paul OHM, « The Argument Against Technology-Neutral Surveillance Laws », (2010) 88-7 *Texas L. Rev.* 1685 ; Daniel GERVAIS, « Towards a New Core International Copyright Norm: the Reverse Three-StepTest », (2005) 9 *Marq. Intell. Prop. L. Rev.* 1, 29.

[54] Ethan KATSH, *The Electronic Media and the Transformation of Law*, New York, Oxford University Press, 1989, p. 189 : « Privacy, like copyright and obscenity, had no direct legal ancestor in the preprint era. »

i) Définition de renseignement personnel

[27] La notion de renseignement personnel est la plus petite unité de base sur laquelle prend appui l'ensemble du Règlement 2012. Sa définition, comme dans la plupart des lois nationales en la matière, se veut inclusive afin d'être susceptible de s'appliquer au plus grand nombre de situations possibles. Le renseignement personnel correspond donc à

> « toute information se rapportant à une personne concernée; »[55]

Nous croyons qu'il importe de ne pas avoir peur de reconnaître que la vision excessivement large, comme l'OCDE l'a d'ailleurs récemment reconnu[56], est susceptible de poser problème. En protégeant à outrance, même des données qui ne présentent aucune sensibilité, qui ont parfois un caractère partiellement ou totalement public, on applique donc un corpus de règles à des informations qui ne mériteraient peut-être pas pareille protection[57] ; on est aussi susceptible de limiter les prérogatives prévues dans d'autres domaines du droit, pour rien. Il est aussi loisible de se demander si cette protection mal ciblée ne fait pas oublier les atteintes véritables qui elles méritent assurément d'être contrôlées, réparées et condamnées. Si nous prenons l'exemple précédemment cité des sites de notation de professeurs, le couplage d'un nom et d'une profession (Vincent Gautrais + professeur) rentre sans aucun doute dans une telle définition de renseignement personnel. Sous réserve de lois qui ont pris le soin de spécifiquement extraire de leur domaine d'application certaines informations publiques presque par essence[58], il ne fait doute qu'une telle information soit assujettie à la loi, et ce, en dépit de son caractère inoffensif. Est-il donc si nécessaire d'appliquer un corpus de règles au complet à des informations si anodines ?

[28] C'est la raison pour laquelle certains auteurs nord-américains vont ajouter une composante implicite à tout renseignement personnel : le dommage. La thèse d'Éloïse Gratton a pris le soin de colliger l'ensemble des auteurs, des textes, qui implicitement ou explicitement, évoquent cette notion comme minimum nécessaire à l'application des lois sur la protection des renseignements

---

[55] Article 4 (2) de la proposition de Règlement 2012. Les amendements Albrecht sont venus complexifier passablement la donne en ajoutant les éléments suivants : « 'personal data' means any information relating to an identified or identifiable natural person ('data subject')**;** an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, unique identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or gender identity of that person; »

[56] OECD, *The OECD Privacy Framework*, p. 114, disponible à http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

[57] Paul OHM, « Broken Promises of Privacy », (2010) 57 *UCLA Law Review* 1701, 1742 ; Daniel J. SOLOVE, « Conceptualizing Privacy », (2002) 90 *California Law Review* 1087 ; Stan KARAS, « Privacy, Identity, Databases », (2002) *American University Law Review* 393.

[58] On peut notamment penser à l'article 2 de la Loi canadienne qui a pris le soin de ne pas considérer comme personnelle l'information relative au travail. Cette disposition a donné lieu à une interprétation rigoureuse. Les lois québécoises n'ont pas opéré une pareille distinction.

personnels[59]. Selon ce courant, il n'y aurait donc lieu d'appliquer ces lois qu'à la condition qu'un risque de dommage prévaut. D'ailleurs, la toute récente proposition de loi canadienne, émanant du principal partie d'opposition, évoque clairement l'existence d'un préjudice[60].

ii) Définition de traitement

[29] En fait, et cette dernière proposition de loi en est l'exemple, la définition de renseignement personnel est intimement liée à celui de traitement qui lui aussi est une opération comprise avec une grande largesse. Toujours dans cette optique de protection optimale, les textes européens ont mis de l'avant cette notion qui correspond à toutes les étapes du cycle de vie du document[61]. Une notion de traitement qui est d'ailleurs absente des lois canadiennes et québécoises qui préfèrent identifier avec plus de finesse l'opération en cause telle que la conservation, la communication, la collecte, etc.[62] Or, chacune de ces étapes ne présentent pas les mêmes risques ; d'une manière générale, et à titre d'exemple, les opérations de divulgation sont susceptibles d'être passablement plus attentatoires que celles de communication interne[63]. Ceci est d'autant plus vrai dans une optique de circulation accrue des données en général et donc des données personnelles en particulier[64]. Présentons l'illustration suivante : un ministère québécois proposa à la population un service d'identification électronique sécurisée. Pour ce faire, l'administré devait saisir une ligne correspondant à une information contenue dans sa déclaration d'impôt, information ensuite vérifiée par les services gouvernementaux. Il faut noter que suite à la vérification, l'information en cause était détruite et ne trouvait plus trace dans le système. Paradoxalement, le consentement qui avait été initié – non sans difficulté afin d'expliciter au citoyen cette opération complexe à laquelle il consentait – était la seule information qui était conservée. Aussi, si une telle opération pourrait ne pas être interprétée comme une communication, il est difficile de croire que cela ne puisse l'être comme un traitement. Notons que dans une hypothèse comme celle-ci, la finalité de l'opération est simple : le service au citoyen. Or, le consentement, qui s'est traduit au mieux dans les faits comme un irritant, au pire comme une source d'angoisse, est le seul pis-aller pour contrer l'utilisation de données personnelles dont il clairement possible d'affirmer que le traitement n'est d'aucun risque pour l'individu.

---

[59] Éloïse GRATTON, *Understanding Personal Information : Managing Privacy Risks*, LexisNexis, Markham (On.), 2013, pp. 208-217.

[60] Proposition de loi C-475, 2013, article 10.01 (1), (2) et (3). Celle-ci est disponible à http://droitdu.net//fichiers/20130409_c_475.pdf.

[61] Cette notion de « cycle de vie » est employée à l'occasion dans les lois relatives à la preuve et à la gestion documentaire. On peut notamment citer au Québec la *Loi concernant le cadre juridique des technologies de l'information*, LRQ c-1-1.

[62] *Loi fédérale sur la protection des renseignements personnels et les documents électroniques*, LC 2000, C-5 ; Loi sur la protection des renseignements personnels dans le secteur privé, LRQ c. P-39.1.

[63] Éloïse GRATTON, *Understanding Personal Information : Managing Privacy Risks*, LexisNexis, Markham (On.), 2013, pp. 219-418.

[64] Vincent GAUTRAIS et Pierre TRUDEL, *Circulation des renseignements personnels et web 2.0,* Éditions Thémis, Montréal, 2010, pp. 19-21.

[30] Ce très rapide survol des notions interreliées de renseignement personnel et de traitement nous montrent que les technologies nouvelles changent la donne en terme de dangerosité et plus exactement dans le difficile équilibre entre efficacité et protection. Parfois une surprotection prévaut ; parfois, des mesures additionnelles doivent être initiées pour contrer les risques d'atteintes[65]. Nous croyons donc que la vision englobante tant sur la définition de renseignements personnels que sur les opérations suivies n'est pas celle qui est susceptible d'assurer la meilleure protection.

B – Consentement

[31] Le Règlement 2012 n'y échappe pas : le consentement y trouve une place de choix, tant dans le corps du texte[66] que dans les considérants[67]. Même si cette condition n'est pas de la toute première heure, certains des premiers textes en matière de protection des renseignements personnels n'y faisant pas mention[68], il a très vite été considéré comme l'outil de souplesse par excellence, l'exception principale qui permet l'utilisation des renseignements personnels. Avant d'analyser comment il est traité dans le Règlement 2012, quelques mots sur l'état des lieux.

i) État des lieux

[32] Le consentement est le moyen principal pour les entreprises et les États d'utiliser, d'user, d'abuser, des renseignements personnels. D'ailleurs, fait symptomatique, les *Facebook*, *Google* et autres plateformes web du monde numérique ne jurent que par lui : nous consentons sur tout ; d'une façon telle qu'il devient impossible de savoir à quoi. Fort de la notion de contrôle précitée, les multinationales insèrent grand nombre de stipulations dont on sait que l'usager moyen ne peut et ne veut connaître : les contrats sont trop longs, trop flous, trop changeants. Le consentement perd donc en pratique son lien originel avec la volonté, ce qui est d'autant plus troublant qu'est apparu une situation de « consent-fetichism »[69], l'acceptation de l'individu étant un blanc-seing pour le contrôleur des données de faire tout et n'importe quoi avec les renseignements personnels. Ceci est d'autant plus grave que si le consentement est requis dans les lois[70], parfois

---

[65] Lyria BENNETT-MOSES, « Recurring Dilemmas : The Law's Race to Keep Up With Technological Change », (2007) 21 *UNSW Law Research Paper*, 4, en ligne : http://ssrn.com/abstract=979861.

[66] L'article 4 (8) dispose : « «consentement de la personne concernée»: toute manifestation de volonté, libre, spécifique, informée et explicite par laquelle la personne concernée accepte, par une déclaration ou par un acte positif univoque, que des données à caractère personnel la concernant fassent l'objet d'un traitement; »

[67] À de multiples reprises, le consentement y est précisé, à savoir aux considérants 25, 31, 32, 33, 34, 40, 41, 53, 55, 58, 86 et 123.

[68] Voir notamment tant les règles de l'OCDE de 1980 (et leurs mises à jour) que la Convention 109 (Principes directeurs pour la règlementation des fichiers informatisés contenant des données à caractère personnel, adoptée le 14 décembre 1990 par l'Assemblée générale des Nations Unies dans sa résolution 45/95 du 14 décembre 1990) de 1990.

[69] Roger BROWNSWORD, « The Cult of Consent : Fixation and Fallacy » (2004) 15 *King's College Law Journal* 223 et 224.

[70] *Loi fédérale sur la protection des renseignements personnels et les documents électroniques*, LC 2000, C-5, Annexe 1, article 4 ; *Loi sur la protection des renseignements personnels dans le secteur privé*, LRQ c. P-39.1, article 13.

avec force, une jurisprudence constante semble valider ces manières de faire[71], et ce, d'une manière passablement plus grave à ce qui nous semble se passer en Europe[72]. Aussi, avant de traiter du Règlement 2012 en particulier, nous voulons nous interroger sur la raison d'être du consentement et la perversion de cette finalité initiale.

[33] En effet, selon nous, alors qu'initialement sa compréhension visait à s'assurer que l'individu ait un **contrôle**[73] sur les informations le concernant, il y a désormais en pratique un glissement vers une acceptation que le gestionnaire de renseignements personnels puisse les utiliser comme il le souhaite, ou presque, dès lors que le premier y a consenti. Il est possible de s'interroger sur cette pratique qui veut que, par le consentement, on ne s'intéresse plus à la protection des renseignements personnels mais à la capacité dont dispose l'individu de refuser, mais plus souvent, d'admettre un certain usage de son espace personnel[74]. Du consentement « protection » s'est donc opéré en pratique un glissement vers le consentement « permission ». Il nous semble donc possible de faire le constat selon lequel il y a lieu, en certains cas, de faire une distinction entre le consentement vu selon une vision généraliste, inspirée du droit des obligations traditionnel, et l'acceptation du même concept en ce qui a trait au droit de la protection des renseignements personnels, sous-catégorie du droit de la personnalité. En effet, les rationalités ne semblent pas les mêmes et nous croyons que dans cette dernière situation il y a

> « a need for a much higher original threshold of consent in privacy law than in contract law »[75].

[34] En premier lieu, la protection des renseignements personnels évoque la gestion d'informations qui correspondent à un certain niveau de sensibilité de par ce lien avec les droits de la personne[76]. Une sensibilité qui impose donc une retenue tant dans l'utilisation que dans la forme assortie au consentement. En second lieu, le consentement semble être un consentement rétractable et qui dispose d'un rapport au temps différent que dans le cadre d'un contrat de vente

---

[71] Vincent GAUTRAIS, « Contrat 2.0 : les 2 couleurs du contrat électronique », *Mélanges Adrian Popovici*, Éditions Thémis, Montréal, 2010, pp. 241-259. On peut bien évidemment citer l'arrêt de la Cour suprême *Dell Computer Corp. c. Union des consommateurs,* 2007 CSC 34.

[72] On peut notamment passer à certaines décisions françaises qui ont considéré que les consentements des sites Amazon était abusifs ou autrement illégaux. À titre d'illustration, on peut citer la décision du Tribunal de grande instance de Paris, première chambre, Section sociale, jugement du 28 octobre 2008, disponible à http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2473.

[73] *Supra*, Partie 1, Paragraphe 1, B, ii).

[74] Steven L. WILLBORN, « Consenting Employees : Workplace Privacy and the Role of Consent », (2006) 66 *Louisiana Law Review* 975, 979.

[75] Ian R. KERR, Jennifer BARRIGAR, Jacquelyn BURKELL et Katie BLACK, « Soft Surveillance, Hard Consent », (2006) 6 *Personally Yours, pp. 1-14*, disponible à http://papers.ssrn.com/sol3/papers.cfm?abstract_id=915407.

[76] Art. 35 du Code civil du Québec, situé dans le Chapitre 3 (Du respect de la réputation et de la vie privée) du Titre 2 (De certains droits de la personnalité) du Livre premier (Des personnes) dudit Code.

par exemple[77]. Même si cela n'apparaît pas expressément dans les définitions mêmes de ce qu'est un consentement[78], il peut être sous-entendu tant de l'esprit des lois sur la protection des renseignements personnels que des dispositions et de leur interprétation, que ce consentement doit être renforcé. À cet égard, les auteurs d'une étude évoquant la situation, guère différente et assurément pas moins protectrice de la loi fédérale, mettent l'accent sur la nature intemporelle du consentement[79].

[35] Cette perception du consentement permet de revisiter l'idée première derrière cette technique législative qu'est le consentement. Et au-delà de sa portée assouplissante pour le gestionnaire des renseignements personnels, elle sous-entend que l'individu est en droit de disposer d'un certain « contrôle » sur ses propres données[80].

[36] A bien des égards, plusieurs principes fondateurs de la protection des renseignements personnels militent pour une même analyse : ainsi, l'accès aux renseignements et la capacité de les corriger voire de les effacer illustre cette capacité de contrôle[81]; même perspective en ce qui a trait à l'obligation de destruction des renseignements personnels dès lors que la finalité pour laquelle ils ont été collectés est remplie[82]; les définitions qui traitent parfois le consentement

---

[77] Néanmoins, et contrairement à la pratique de certains organismes, il a été déjà jugé qu'un consentement n'a pas besoin d'être récent et tant qu'il n'est pas révoqué, il est toujours valide. *X c. Québec (Société de l'assurance automobile)* décision non rapportée, CAI, no PP 98 09 09, 9 décembre 1999) Doray, III/59-19.

[78] À la différence de la *Loi fédérale sur la protection des renseignements personnels et les documents électroniques*, article 4.3.8. de l'annexe 1 : « ne personne peut retirer son consentement en tout temps, sous réserve de restrictions prévues par une loi ou un contrat et d'un préavis raisonnable. L'organisation doit informer la personne des conséquences d'un tel retrait. »

[79] Ian R. KERR, Jennifer BARRIGAR, Jacquelyn BURKELL et Katie BLACK, « Soft Surveillance, Hard Consent », (2006) 6 *Personally Yours, pp. 1-14*, page 5, disponible à http://papers.ssrn.com/sol3/papers.cfm?abstract_id=915407: « *PIPEDA*'s consent model is best understood as providing ***an ongoing act of agency*** to the information subject and is a much more robust than the usual model for consent in private law which treats consent as an isolated moment of contractual agreement during an information exchange. (…) Organizations wishing to use personal information must obtain the ***ongoing consent*** of the information subject for **continued use**. In other words, the ***continued use*** of personal information must be understood as a necessary consequence of the information subject's ***continuing consent*** to its use and not merely as a consequence of the initial consent to collect the information. » (Nos soulignements)

[80] Ian R. KERR, Jennifer BARRIGAR, Jacquelyn BURKELL et Katie BLACK, « Soft Surveillance, Hard Consent », (2006) 6 *Personally Yours, pp. 1-14*, page 5, disponible à http://papers.ssrn.com/sol3/papers.cfm?abstract_id=915407: « *PIPEDA* generally allows the information subject to withdraw consent at any time. *PIPEDA* is predicated on the notion that individuals **have a *right* to control personal information** about them. This ongoing right of control is reinforced in law by the corollary requirement of ongoing consent codified in Principle 4.3.8 of *PIPEDA*. Consequently, unless they surrender it, individuals retain ultimate control over their personal information and can withdraw consent at any time. » (Nos soulignements)

[81] Nous pouvons citer par exemple l'article 76 de la *Loi sur l'accès et la protection de renseignements personnels dans le secteur public*, LRQ A 2.1.

[82] Nous pouvons citer dans cette hypothèse l'exemple de l'article 73 de la la *Loi sur l'accès et la protection de renseignements personnels dans le secteur public*, LRQ A 2.1.

d'une façon telle qu'on « ne trouve guère de parallèle dans les Codes civils usuels »[83]. À cet égard, l'analogie proposée par les auteurs Kerr et suivants avec le contrat de « licence » est fort à propos[84] : le consentement visant à déterminer la circulation des renseignements personnels est l'équivalent de ce contrat *sui generis* qui ne constitue qu'un droit d'usage et non une cession de la propriété de l'œuvre.

ii) État du droit

[37] Dans ces propositions de règlements, on découvre une volonté manifeste d'encadrer ces pathologies contractuelles. Plusieurs de ces tentatives nous apparaissent fort prometteuses et une source d'inspiration évidente. Avec égard, le salut que nous apercevons dans ces textes ne provient pas de la définition que l'on trouve à l'article 4 (8) du Règlement 2012[85] ; sa généralité, son lien avec le caractère explicite, ne nous apparaît pas être la solution la plus protectrice en toutes situations. Il est en effet de multiples hypothèses où les consentements tiennent lieu de l'évidence, le recours à cet outil n'étant qu'une source de distraction, de complexification[86].

[38] Néanmoins, il importe de signaler l'avancement indiscutable que semble être l'article 7 (4) qui prévoit les hypothèses de consentement exorbitant tel celui qui se fait à l'occasion d'une recherche d'emploi[87] : certains employeurs ne manquent pas en effet de demander à l'employé potentiel de donner accès à sa page *Facebook* afin de voir qui il est vraiment. Cela semblerait désormais impossible ; du moins, si les amendements Albrecht n'étaient pas venus changer considérablement la donne[88]. Également, il est intéressant que l'on requiert pour les données

---

[83] François RIGAUX, « Libre circulation des données et protection de la vie privée dans l'espace européen », dans Pierre TABATONI, *La protection de la vie privée dans la société d'information*, tome 2, 2000, Presses universitaires de France, 2000, disponible en ligne à < http://www.asmp.fr/travaux/gpw/internetvieprivee/rapport2/chapitr8.pdf >.

[84] Ian R. KERR, Jennifer BARRIGAR, Jacquelyn BURKELL et Katie BLACK, « Soft Surveillance, Hard Consent », (2006) 6 *Personally Yours, pp. 1-14*, page 6, disponible à http://papers.ssrn.com/sol3/papers.cfm?abstract_id=915407. Les auteurs affirment notamment : « Taken altogether, the consent provisions in *PIPEDA* strongly suggest that consent acts like a "license" that permits some *limited* collection, use, or disclosure. Thus, the consent given to an organization to use an individual's personal information is necessarily restricted and *does not* give the organization ultimate control over personal information in perpetuity. »

[85] « consentement de la personne concernée » : toute manifestation de volonté, libre, spécifique, informée et explicite par laquelle la personne concernée accepte, par une déclaration ou par un acte positif univoque, que des données à caractère personnel la concernant fassent l'objet d'un traitement; »

[86] À titre d'exemple, lorsqu'un site faisant la promotion du tourisme d'une ville, d'une région ou d'un pays offre la possibilité aux individus de déposer des contenus, les sites s'assurent que la collecte des données est consentie par les individus. Or, il n'y a pas collecte mais dépôt volontaire de la part des personnes physiques. Pour reprendre l'analogie utilisée dans un précédent ouvrage (Vincent GAUTRAIS et Pierre TRUDEL, *Circulation des renseignements personnels et web 2.0,* Éditions Thémis, Montréal, 2010, p. 187), cela peut être assimilée à l'individu qui se rend chez un médecin pour une prise de sang et qui consent à ce que celle-ci soit faite.

[87] « 7(4). Le consentement ne constitue pas un fondement juridique valable pour le traitement lorsqu'il existe un déséquilibre significatif entre la personne concernée et le responsable du traitement. »

[88] La nouvelle disposition issue des amendements Albrecht laisse pantois ! (4. Consent shall be purpose-limited and shall lose its validity when the purpose ceases to exist or as soon as the processing of personal data is no longer necessary for carrying out the purpose for which they were originally collected. The execution of a contract or the

concernant des enfants le consentement de celui qui est le titulaire de l'autorité parentale, et ce, de manière très similaire à ce qui prévalait dans la loi américaine Coppa (*Children Online Privacy Protection Act)*[89]. Non sans difficultés applicatives.

[39] Une autre « invention » fort intéressante que l'on puis trouver est l'aménagement d'un consentement « image » qui découlent des amendements Albrecht. Dans le nouvel article 13A, il est en effet prévu que certaines politiques doivent désormais utiliser une forme standardisée à l'aide de pictogrammes. Ainsi, fort des explications qu'ils autorisent, une image valant parfois mille mots, on est en mesure d'attendre un consentement en connaissance de cause. Cette approche très novatrice nous apparaît avoir un vrai potentiel de protection. La lecture des écrans est en effet fort différente de celle qui prévaut sur un support papier ; le processus d'accès à l'information ne suit pas forcément le même caractère linéaire. L'œil butine, s'égare, se trompe davantage[90]. Or, un moyen de contrer cette perte de lisibilité est l'utilisation d'images qui sont particulièrement adaptées à l'écran. L'expérience fut par exemple suivie pour les contrats *creative commons* avec, nous semble-t-il, pas mal de bonheur[91]. D'ailleurs la Commission d'accès à l'information du Québec proposa récemment une même solution[92].

[40] Toujours sur la forme, les amendements Albrecht ont pris le soin d'ajouter à l'article 11 le qualificatif de concision[93]. Au-delà des idéaux de transparence, de connaissance explicite, cette obligation de faire court est en effet le meilleur moyen de d'assurer d'un accès véritable aux contenu auquel le citoyen s'oblige. Il est vrai, que si l'on voit les nouvelles pratiques récentes, comme sur la plateforme *Facebook*, si la tendance est au raccourcissement des contrats, celle-ci se traduit par une multiplication des pages. Ce qui n'est pas mieux…

2 – Solutions processuelles

[41] Mais au-delà des solutions substantielles, des principes fondamentaux qui constituent la trame conceptuelle de la protection des renseignements personnels en général, il nous apparaît

---

provision of a service shall not be made conditional on the consent to the processing of data that is not necessary for the execution of the contract or the provision of the service pursuant to Article 6(1), point (b).) Au-delà d'une logorrhée bien peu salutaire, il semble que le caractère abusif de certaines situations ne donnent plus lieu à interdiction formelle. En effet, l'employeur qui demande un accès au compte *Facebook* d'un employé potentiel exige un consentement en lien à une finalité qui ne laisse aucun doute. Or, en pareille circonstance, ce n'est pas le doute quant à la finalité qui posait problème mais bien le caractère grossièrement abusif, déséquilibré, de la requête. Ce glissement nous apparaît bien triste.

[89] La loi est disponible à <http://www.coppa.org/coppa.htm>, Section 1302, n° 9.

[90] Jakob NIELSEN, « Writing for the Web », (1997) disponible à <http://www.nngroup.com/articles/be-succinct-writing-for-the-web/>.

[91] Vincent GAUTRAIS, « Les contrats de cyberconsommation sont presque tous illégaux ! », (2005) *Revue du Notariat*, 617-650.

[92] COMMISSION D'ACCES A L'INFORMATION DU QUEBEC, *Rapport quinquennal 2011 – Technologies et vie privée à l'heure des choix de société*, 2011, p. 24, disponible à < http://www.cai.gouv.qc.ca/documents/CAI_RQ_2011.pdf >.

[93] Article 11 (1) : « 1. The controller shall have concise, transparent, clear and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights. »

que les changements principaux en la matière sont bien davantage d'ordre procédural. En fait, depuis quelques années, une sorte de consensus semble s'être établi selon lequel la complexité peut être gérée en évaluant la diligence avec laquelle le responsable du traitement (ce qui se traduit en anglais dans les amendements Albrecht par « controller ») s'emploie dans son ouvrage. Sous l'appellation d'imputabilité, plus connue encore en anglais par le terme d' « accountability », la question est donc bien plus « Qui » que « Quoi ». Aussi, nous aimerions développer quelque peu la notion de documentation et plus généralement celle de la gouvernance en matière de vie privée.

A – Documentation

[42] Les technologies de l'information, presque par essence, nous demandent de repenser la manière de les gérer. Alors que le papier détient souvent des garanties liées au caractère physique de son support, les documents électroniques en exigent d'autres qui sont extérieures au document lui-même. Comme le mentionnait le professeur Katsh, « Paper contract is an act ; electronic contract is a process. »[94]. Aussi, plutôt que de s'attaquer en amont aux données, il importe assurément au responsable des données d'offrir des garanties supplémentaires quant au traitement en aval qu'il est possible d'en faire[95]. De plus en plus donc, celui-ci doit monter une documentation qui va permettre d'évaluer la diligence employée pour assurer la protection des renseignements personnels. Cette notion de documentation est d'ailleurs inhérente à la *Loi*

[94] Ethan KATSH, *Law in a Digital World*, New York, Oxford University Press, 1995, p. 129.

[95] Daniel J. WEITZNER, Harold ABELSON, Tim Berners-Lee, Joan FEIGENBAUM, James HENDLER et Gerald Jay SUSSMAN, « Information Accountability », disponible à http://dspace.mit.edu/bitstream/1721.1/37600/2/MIT-CSAIL-TR-2007-034.pdf. On peut notamment citer l'extrait suivant : « This paper argues that debates over online privacy, copyright, and information policy questions have been overly dominated by the access restriction perspective. We propose an alternative to the "hide it or lose it" approach that currently characterizes policy compliance on the Web. Our alternative is to design systems that are oriented toward information accountability and appropriate use, rather than information security and access restriction. In a world where information is ever more easily copied and aggregated, and where automated correlations and inferences across multiple databases can uncover information even when it has not been explicitly revealed, accountability must become a primary means by which society addresses issues of appropriate use. Our goal is to extend the Web architecture to support transparency and accountability. When information has been used, it should to possible to determine what happened, and to pinpoint use that is inappropriate. This requires augmenting Web information with data about provenance and usage policies, and creating automated means for maintaining that provenance and interpreting policies. Transparency and accountability can be supported by a set of technical mechanisms we call Policy Awareness. Policy Awareness is a property of information systems that provides all participants with accessible and understandable views of the policies associated with information resources, provides machine-readable representations of policies in order to facilitate compliance with stated rules, and enables accountability when rules are intentionally or accidentally broken. Our understanding of the dilemmas of information policy in the age of the Web is built upon the work of numerous legal academics and writers. Our proposed public policy and systems architecture framework is an effort integrate these insights into a comprehensive framework of law and technology that, while not immediately providing answers to all legal or technical design questions, sets out a direction in which we are likely see the Web and other large-scale systems evolve toward greater accountability. »

fédérale sur la protection des renseignements personnels et les documents électroniques[96] et elle fit son chemin en Europe également[97].

[43] Et le Règlement 2012 reprend allégrement la notion. En fait, si le concept est loin d'être neuf[98], elle est clairement identifiée comme la solution à suivre pour s'assurer d'une meilleure protection. L'article 28 du Règlement 2012 précise donc l'obligation de documentation[99], en prenant soin, d'une part, d'identifier huit types d'informations distinctes et, d'autre part, de « botter en touche » en autorisant la commission de proposer des formes documentaires particulières. Le Règlement 2012 vise bien à « l'instauration d'une responsabilité globale du responsable du traitement »[100].

[44] Au-delà de cette disposition, c'est bien le rôle du responsable de traitement qui prend du gallon. En premier lieu, si son statut était déjà bien représenté dans la directive de 1995, il nous apparaît désormais avoir à accomplir un rôle durant tout le « cycle de vie » du document qui supporte des renseignements personnels. **Avant** le traitement des données, une analyse de risque peut être envisagée[101]. **Après**, un renforcement important des mesures est exigée avec notamment une obligation de déclaration lorsqu'un bris de confidentialité survient, nécessitant à la fois une action auprès de l'autorité nationale mais aussi envers les individus concernés. Notons que cette démarche de notification est également prévue dans une récente proposition de loi canadienne[102] et qu'elle s'opère dans les faits déjà de façon volontaire de la part de certaines entreprises canadiennes. Quant à l'obligation d'avertir les individus en cause (Article 32), et ce même si la démarche est forcément susceptible de les effrayer, il n'en demeure pas moins que c'est souvent le meilleur moyen de mitiger les dommages, l'intéressé étant le plus à même d'apercevoir les éventuelles conséquences de la divulgation non maîtrisée. Évidemment, c'est **pendant** la durée de vie utile du document que l'action principale du responsable du traitement s'opère. Que ce soit en ce a qui a trait à la communication, à l'accès qui doit être laissé à

---

[96] Voir notamment l'annexe 1 et ses multiples références aux notions de documentation, de politiques et procédures, etc. Cette même annexe dispose aussi explicitement d'un article sur le sujet (article 1).

[97] GROUPE DE TRAVAIL ARTICLE 29, « Avis n°3/2010 sur le principe de la responsabilité », 00062/10/FR, adopté le 13 juillet 2010.

[98] Le principe selon lequel il importe pour un responsable des renseignements personnels de documenter ses manières de faire était notamment déjà présent dans les lignes directrices de l'OCDE de 1980.

[99] Article 28 (1) : « Chaque responsable du traitement et chaque sous-traitant ainsi que, le cas échéant, le représentant du responsable du traitement, conservent une trace documentaire de tous les traitements effectués sous leur responsabilité. »

[100] Règlement 2012, p. 12.

[101] Règlement 2012, article 33. Notons que cette obligation existe déjà au Canada dans certains secteurs et notamment le secteur public. C'est le cas avec un Règlement qui vaut au Québec (Règlement sur la diffusion de l'information et sur la protection des renseignements personnels, c.A-2.1, r. 0.2) ; c'est aussi vrai au niveau fédéral mais sur la base d'une norme informelle qui n'a pas force de loi (COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE AU CANADA, Rapport de vérification : évaluation des facteurs relatifs à la vie privée des programmes, plans et politiques, 2007, disponible à < https://www.priv.gc.ca/information/pub/ar-vr/pia_200710_f.pdf >).

[102] Projet de loi C-475, 2013, article 10.01 (2), disponible à < http://droitdu.net//fichiers/20130409_c_475.pdf >.

l'intéressé, à la conservation des données, et plus généralement à l'ensemble des opérations qui compose le traitement.

[45] En second lieu, la documentation va donner lieu à une sanction véritable. D 'abord, une évaluation de la part de l'autorité nationale aura pour objet de vérifier sa suffisance, la documentation devant être transmise à l'autorité de contrôle[103]. Si les règles d'imputabilité ont souvent distingué l'audit interne et externe[104], on est ici clairement dans une hypothèse où une surveillance extérieure prévaut. Ensuite, la protection des renseignements personnels entre dans une ère nouvelle, à savoir celle d'un droit plein et entier qui donne lieu à des sanctions administratives dissuasives[105]. Ce constat envieux est encore une fois d'autant plus facile à faire que notre système canadien est d'une incroyable faiblesse à cet égard[106].

B – Gouvernance communautaire

[46] l'avènement de la documentation correspond à une obligation du responsable du traitement lui-même. Il s'agit donc d'une approche individuelle où il identifie, sur la base d'une trame élaborée dans le Règlement 2012, les obligations auxquelles il s'oblige. Dans une certaine mesure, le responsable du traitement « légifère » sur son propre sort ; il est le principal acteur de son cadre normatif. Mais il y a autre chose : le Règlement 2012 met de nouveau l'accent sur un pouvoir de délégation de la Commission qui devra élaborer des normes plus précises quant à la façon dont la documentation va se matérialiser[107]. Conformément à un processus qui est déjà fort courant, notamment dans le monde de la sécurité documentaire, il y a lieu de favoriser des productions normatives qui soient aptes à mieux gérer la complexité. Entre normes formelles et contrats, il existe donc une place pour des normes qui puissent s'immiscer entre eux deux.

[47] Une place qui est d'autant plus importante de combler que le débat sur la protection des renseignements personnels s'internationalise de plus en plus. La pression est mise sur des entreprises internationales et la mise en commun des États est souvent un moyen plus efficace de

---

[103] Règlement 2012, article 28 (3).

[104] Richard MULGAN, « Accountability : An Ever-Expanding Concept?., dans Public Administration (2000), 78, 3, pp. 556, 562 : « a sufficiently robust distinction can still be maintained between having to account to someone else for one's actions and not having to do so » ; Colin BENNETT, « International Privacy Standards : Can Accountability ever be Adequate? », dans *Privacy Laws & Business International Newsletter* , n°106, août 2010, p. 22.

[105] Règlement 2012, article 79 (5) f) : « L'autorité de contrôle inflige une amende pouvant s'élever à 500 000 EUR ou, dans le cas d'une entreprise, à 1 % de son chiffre d'affaires annuel mondial, à quiconque, de propos délibéré ou par négligence: (…)ne tient pas, ou pas suffisamment, à jour la documentation conformément à l'article 28, à l'article 31, paragraphe 4, et à l'article 44, paragraphe 3; »

[106] Allocution prononcée par Jennifer STODDART : « Protéger plus efficacement la vie privée des Canadiennes et des Canadiens », Commentaires présentés au Centre de recherche en droit, technologie et société de l'Université d'Ottawa. Le 19 janvier 2011, Ottawa (Ontario) en ligne < http://www.priv.gc.ca/media/sp-d/2011/sp-d_20110119_f.asp >.

[107] Règlement 2012, article 28 (5).

faire infléchir leurs comportements. Quelques initiatives virent le jour[108], avec un certain bonheur croyons nous[109], et ce, même si elles présentent évidemment un caractère obligatoire bien moindre. Certes, en certains cas, cette approche informelle fonctionne et permet que des comportements soient corrigés, l'atteinte à la réputation que pourrait devoir supporter une entreprise récalcitrante n'étant pas à négliger[110]. Néanmoins, cette hypothèse ressemble davantage à une situation d'autorégulation, correspondant peut-être moindrement à une tradition européenne sans doute plus formelle[111]. La solution qui apparaît avoir été privilégiée dans le Règlement 2012 s'apparente à la situation classique d'une délégation réglementaire et non à une telle hypothèse.

[48] C'est donc fort de cette coloration culturelle que nous croyons pourtant que cette voie communautaire n'est pas sans atouts et aurait pu, aurait du, être essayée en matière de gouvernance de la protection des renseignements personnels. Gouvernance. Le mot est lâché ! On ne sait trop ce qu'il représente et pourtant, depuis les années 1990, cette notion ancienne a été remise au goût du jour dans plusieurs domaines du droit. Appliquée aux technologies de l'information, la définition de ce terme tient du pléonasme, l'étymologie de « gouvernance » et de « cyber » relevant dans les deux cas de la même racine grecque « kubernân » signifiant « piloter ». Gouvernance du cyberespace, voudrait donc dire gouverner ce qui est gouverné.

[49] Face à la nébulosité de ce terme à la mode, originant de cercles internationaux (ONU, Banque mondiale, FMI, etc.), il est pour le moins possible d'identifier une des raisons d'être de ce néologisme « mou », imprécis. Justement, l'absence de tradition associée à ce terme traduit une volonté inclusive visant à fédérer les différentes formes de droit. En effet, derrière cette incapacité définitionnelle, il existe assurément une quête d'intégrer différentes formes de régulation que la complexité des univers contemporains présente. Aussi, au regard du format du présent papier, nous allons éluder la tentative définitionnelle associée à ce terme pour nous cantonner à une question, une seule, la plus importante dans le monde des technologies de l'information selon David Post[112] : qui ? Qui régule ? qui gouverne ?

---

[108] On peut par exemple penser aux « Madrid international privacy standards » disponibles à < http://www.justice.gov.il/NR/rdonlyres/F8A79347-170C-4EEF-A0AD-155554558A5F/24464/20091.pdf >, et traités par Colin BENNETT, « International Privacy Standards : Can Accountability ever be Adequate? », dans *Privacy Laws & Business International Newsletter* , n°106, août 2010, p. 22. Accord du forum de la Coopération économique de la zone Asie-Pacifique APEC Privacy Framework, Preamble, 2005, en ligne à http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx.

[109] Charles RAAB, « The Meaning of 'Accountability' in the Information Privacy Context », dans Managing Privacy through Accountability, Palgrave Macmillan, 2012, p. 11.

[110] On peut notamment penser à la publicité comportementale que *Google* effectuait au Canada et qui donna lieu à une correction suite à une négociation avec le Commissariat à la vie privée. *Supra*, Partie 1, Paragraphe 2, A, s'intitulant « Choix normatif ».

[111] James Q. WHITMAN, « The Two Western Cultures of Privacy : Dignity versus Liberty », (2004), 113 *Yale Law Journal* 1151.

[112] David POST, « Anarchy State and the Internet », (1995) *Journal of Online Law article* 3, disponible à http://papers.ssrn.com/sol3/papers.cfm?abstract_id=943456.

[50] À cette question, encore une fois, et au-delà de l'intervention naturelle de l'État, nous croyons qu'une communauté donné est susceptible d'être un producteur de normes. Dès lors que le dialogue entre des entités du secteur privé et du secteur public rempli un certain nombre de conditions, il n'y a pas selon nous d'empêchement à l'existence d'une norme informelle qui puisse avoir une certaine effectivité, voire une reconnaissance judiciaire. Cette reconnaissance a en effet déjà été reconnue même dans des domaines à forte saveur d'ordre public[113]. Une telle réception juridique bien évidemment devra se baser sur une approche pluraliste du droit et assurément moindrement positiviste. Elle nécessitera aussi de revoir la portée traditionnellement contractuelle qui est associée à la notion d'usage en droit civil[114]. L'intégration des normes informelles dans le giron du droit de la protection des renseignements personnels n'est pas encore maîtrisée tant les perceptions divergent selon les auteurs, les cultures juridiques et eu égard à la grande variété des modèles possibles. Il existe aussi un certain nombre de normes dont on peut douter de la recevabilité étant donné que leur accointance avec certains groupes d'intérêts ou le caractère mercantile de leur production[115], posent problème. Néanmoins, au-delà de ces irritants, la flexibilité que ces modèles normatifs autorisent nous apparaît source à un réel potentiel. Pour ce, les conditions de reconnaissance de telles normes informelles doivent être étudiées, identifiées. Et au-delà de celles qui sont habituellement associées aux usages, telles que la fréquence, l'uniformité, la raisonnabilité, l'ancienneté[116], des critères qualitatifs davantage associés non pas aux normes elles-mêmes mais à leur processus de création devraient être mis de l'avant. Ainsi, des normes informelles en matière de protection de renseignements personnels pourraient être reconnues sous réserve de qualités telles que la représentativité, la légitimité de l'ordre juridique en charge de leur élaboration, la qualité du dialogue entre des groupes d'intérêts concurrents[117].

[51] Justement à propos de dialogue, la conclusion que nous pourrions apporter au présent document est que d'un continent à l'autre, des différences existent dans ce domaine à forte saveur culturelle et qu'il importe d'échanger à ce sujet. La première étape est pour le moins de les appréhender, et ce, même si le clivage que nous avons peut-être tracé est moins subtil que celui qu'il est vraiment. En second lieu, nous avons fait état de divergences qui, bien que réelles, portent peut-être sur des problématiques qui ne sont pas les plus importantes ; les plus

---

[113] On peut notamment penser à l'arrêt de la Cour suprême *Dell Computer Corp. c. Union des consommateurs,* 2007 CSC 34 où en matière de consommation on pris appui, notamment, sur certains codes de conduite élaborés avec l'industrie.

[114] Vincent GAUTRAIS, *La neutralité technologique : rédaction et interprétation des lois face aux technologies*, Montréal, Éditions Thémis, 2012, p. 117.

[115] À titre d'illustration, nous sommes parfois quelque peu suspicieux vis-à-vis de certaines normes ISO dont la provenance originelle devrait pourtant être sujette à caution. Néanmoins, et pour reprendre l'expression de mon collègue Vermeys (Nicolas VERMEYS, *Responsabilité civile et sécurité informationnelle*, Cowansville, Éditions Yvon Blais, 2010, p. 128.), il y a une vraie « industrie des normes » qui au-delà de leur caractère payant, ne sont que des copier / coller d'autres normes nationales, le tout avec parfois une vacuité assez surprenante en terme de contenu.

[116] Jean-Claude ROYER, La preuve civile, 4e éd., Cowansville, Éditions Yvon Blais, 2008, par. 108) qui définit les usages de la façon suivante : « Règle qui s'est formée par une pratique constante, répétée, publique, uniforme et générale à laquelle les parties intéressées ont donné une force obligatoire. »

[117] Vincent GAUTRAIS, *La neutralité technologique : rédaction et interprétation des lois face aux technologies*, Montréal, Éditions Thémis, 2012, p. 119.

dangereuses pour le citoyen. Aussi, si des oppositions parfois frontales existent sur des situations qui nous semblent pourtant peu sujettes à dommage, il n'en demeure pas moins que la protection des renseignements personnels relève actuellement et demain encore davantage d'une sensibilité réelle. En troisième lieu enfin, il y a dans ce débat autour de la protection des renseignements personnels un questionnement qui nous semble encore passablement adolescent, tant la nouveauté de la matière que le caractère changeant du cadre d'analyse n'autorisent guère à beaucoup de certitudes.