Cahiers de recherche sociologique

L'informatique et les droits des personnes

René Laperrière

Numéro 21, 1993

L'innovation technologique

URI : https://id.erudit.org/iderudit/1002220ar
DOI : https://doi.org/10.7202/1002220ar

Aller au sommaire du numéro

Éditeur(s)

Département de sociologie - Université du Québec à Montréal

ISSN

0831-1048 (imprimé)
1923-5771 (numérique)

Découvrir la revue

Citer cet article

Laperrière, R. (1993). L'informatique et les droits des personnes. *Cahiers de recherche sociologique*, (21), 53–77. https://doi.org/10.7202/1002220ar

Résumé de l'article

Les nouvelles technologies de l'information et des communications posent des problèmes sociaux inédits, particulièrement en ce qui concerne la protection de la vie privée des personnes. Elles donnent naissance à une société de surveillance généralisée et ajoutent aux moyens de contrôle social. En transformant le droit et sa pratique, elles peuvent contribuer à aggraver les inégalités devant la loi. La réglementation ne suffit pas à enrayer l'accumulation et la diffusion incontrôlées des renseignements : elle doit être complétée par des arrangements contractuels et des initiatives non juridiques faisant appel à la participation des décideurs et des citoyens, et conduisant à une redéfinition des rapports sociaux entre individus, corporations et État.

Cahiers de recherche sociologique, no 21, 1993

L'informatique et les droits des personnes

René LAPERRIÈRE

Les innovations technologiques accélérées des vingt dernières années ont conduit, entre autres développements, à l'introduction des ordinateurs et des moyens de télécommunications dans de multiples secteurs d'activité. Or, si la majorité des juristes se sont surtout concentrés sur les problèmes des décideurs, particulièrement la protection de leurs ordinateurs, de leurs logiciels et de leurs communications[1], les intervenants sociaux ont été plus préoccupés dans leur ensemble par les effets de ces innovations sur les droits et libertés des personnes. Ainsi, parallèlement à la constitution de vastes banques de données et à la mise en place de systèmes de diffusion instantanée de ces renseignements, des voix se sont élevées de milieux très divers pour lancer des avertissements et réclamer des autorités publiques l'adoption de mesures juridiques de protection des droits et libertés des individus face aux usages incontrôlés de ces nouvelles technologies dont les conséquences ne pouvaient être prévues lorsque les normes et recours juridiques existants avaient été institués.

Cette vision un peu romantique de l'évolution du droit dans ce domaine doit être tempérée par la prise en considération du rôle des développeurs de systèmes eux-mêmes et des grands usagers de ces systèmes, qui ont quelquefois réagi à titre personnel pour promouvoir une protection même minimale des droits des personnes ou de leurs attentes en termes de vie privée et de traitement équitable, mais qui ont aussi démontré l'intérêt de leurs organisations à ce que les investissements consentis dans les nouvelles technologies soient protégés dans la mise en place de systèmes répondant à des normes officielles qui ne seraient pas remises en question dans un avenir trop rapproché. Et de façon plus générale, les problèmes inédits posés par les multiples innovations technologiques ont forcé les juristes et les décideurs à réfléchir sur les solutions normatives et institutionnelles à y apporter et sur la capacité effective du système juridique à intégrer ces solutions. On a donc assisté à un double phénomène d'émergence et de non-émergence de normes, de procédures et d'institutions pour gérer l'innovation ou au contraire pour la laisser se développer sans aucune forme de contrôle public.

---

[1] Voir par exemple J.P. Chamoux, *Menaces sur l'ordinateur*, Paris, Seuil, 1986, 225 p.

Notre propos se limitera ici à traiter de l'informatisation dans la perspective de la défense et de la promotion des droits et libertés des personnes. Après avoir examiné les problèmes socio-juridiques posés par les progrès de l'informatique et des télécommunications, nous ferons état des diverses solutions juridiques ou autres mises en place pour y répondre, et terminerons sur les enjeux actuels que posent au droit l'extension et l'approfondissement de l'informatisation.

I Les problèmes posés par l'informatisation

Les premiers problèmes que l'informatisation généralisée crée pour les personnes ont trait à la protection de leur vie privée. Mais l'on s'est aperçu assez rapidement que la protection des droits des personnes dans tous les milieux de vie allait de pair avec leur capacité d'intervenir politiquement et socialement, et de résister à la mise en place de systèmes de surveillance et de contrôle social. Sur le plan du droit et de l'administration de la justice, l'informatisation commence aussi à poser des problèmes inédits qui iront en se multipliant.

1.1 La protection de la vie privée

Si la vie privée reste une notion mal définie[2], les atteintes auxquelles elle est exposée se sont tellement multipliées grâce aux technologies nouvelles que les spécialistes et la population en général sont d'avis qu'elle ne peut plus être protégée adéquatement de nos jours[3]. Le débat sur les dangers sociaux de l'informatisation s'est en grande partie confondu avec celui de la protection de la vie privée. Ces agressions, qui ne sont quelquefois que des manifestations de modes de gestion sociale plus transparents, plus publics, prennent des formes inédites parce que les technologies d'aujourd'hui permettent de commettre à grande échelle et en profondeur des indiscrétions dans la vie intime des individus, ou plus banalement d'établir des portraits des comportements des personnes et de groupes entiers, à toutes sortes de fins. On a constaté que les atteintes à la vie privée

---

[2] Dès 1890, deux célèbres juristes américains avaient défini la *privacy* comme étant "le droit d'être laissé seul" ou en paix: S. Warren et L. Brandeis, "The Right to Privacy", *Harvard Law Review*, no 4, 1890, p. 193. Dans un monde en croissante interaction, elle porte désormais sur l'autonomie qu'une personne (et même par extension un groupe) est en droit d'avoir dans les choix concernant sa vie personnelle, celle de sa famille, et ses rapports avec autrui: voir le mot "privacy" dans: *Black's Law Dictionary*, 5e éd., 1979, p. 1075-1076.

[3] Citons quelques ouvrages marquants: J.B. Rule, *The Politics of Privacy, Planning for Personal Data Systems as Powerful Technologies*, New York, Elsevier, 1980; M.R. Rubin, B. Dervin (dir.), *Private Rights, Public Wrongs: The Computer & Personal Privacy*, Ablex Pub., 1989.

variaient selon les types d'activité, leur lieu, leurs finalités, le statut des personnes, ou les moyens techniques utilisés[4].

Le secteur privé

Un premier constat: alors que les principales menaces identifiées depuis les années soixante provenaient du secteur public, autant de la surveillance policière et des services secrets que de la constitution de vastes fichiers des populations, on a pu remarquer depuis une dizaine d'années, et surtout depuis la fin de la guerre froide et l'importance accrue donnée au commerce par rapport au militaire, que le secteur privé dispose maintenant de banques de renseignements personnels tout aussi imposantes que celles du public, et que les grands organismes publics et privés s'échangent désormais des millions de renseignements de façon routinière[5].

Les télécommunications

Les télécommunications se sont développées à un rythme aussi fulgurant que l'informatique, et les deux technologies ont rapidement été intégrées pour permettre non seulement aux ordinateurs de communiquer entre eux, mais aussi d'effectuer à distance la collecte de données ultérieurement traitées par ordinateur et rediffusées dans des réseaux de plus en plus étendus. Si l'écoute électronique avait déjà mis l'industrie des télécommunications sur la sellette, les batailles les plus récentes se sont faites autour des systèmes d'identification des appels (*caller ID*), qui posent des difficultés particulières aux personnes qui logent des appels au gouvernement, ou qui cherchent à communiquer avec leur famille à partir de refuges pour femmes battues, ou encore qui souhaitent bénéficier du secret professionnel en communiquant avec leur médecin ou leur avocat.

L'encodage des messages qui transitent sur les voies de télécommunications a fait l'objet de vives contestations, autant des individus que des entreprises privées,

---

[4] L'ouvrage classique sur le sujet qui a lancé le débat et suscité l'adoption à terme de la loi américaine est de A.F. Westin, *Privacy and Freedom*, New York, Atheneum, 1967. Une vaste étude avait aussi précédé cette adoption: United States Congress, Privacy Protection Study Commission, *Personal Privacy in an Information Society: Report of the Commission*, Washington, US Gov. Printing Office, 1977, 654 p. Sur les diverses articulations de cette notion de vie privée et ses enjeux juridiques, voir: R. Laperrière et P. Patenaude, "Les atteintes à la vie privée", dans S. Langlois, F. Dumont et Y. Martin (dir.), *Les problèmes sociaux du Québec,* Institut québécois de recherche sur la culture, nov. 1993 (sous presse).

[5] Sur toute cette question, voir Groupe de recherche informatique et droit, *L'identité piratée. Étude sur la situation des bases de données à caractère personnel dans le secteur privé au Québec et sur leur réglementation en droit comparé et international,* Montréal, Société québécoise d'information juridique, 1986, 363 p.

lorsque les agences publiques de renseignement telles que le FBI et le NSA américains ont voulu faire maintenir un monopole des services secrets sur les codes sous prétexte de permettre le contre-espionnage et la recherche des criminels. Or, dans un contexte où le besoin de sécurité des communications privées va grandissant et où il est devenu impossible de contrôler les communications, l'industrie a fait savoir au gouvernement qu'elle perdrait d'importants contrats si le nouveau standard de chiffrement (*encryption standard*) que l'on voulait vendre au monde entier pouvait être violé par les services secrets américains.

Ce sont aussi les télécommunications qui permettent le plus facilement de se procurer des renseignements personnels pour les faire servir à des usages secondaires étrangers aux fins pour lesquelles ils avaient été divulgués et recueillis à l'origine. La vente de renseignements dérivés est devenue une véritable industrie, qui offre des services intégrés de marketing et de gestion de bases de données. Dans cette évolution, les intérêts commerciaux des propriétaires et des intermédiaires ont tendance à obtenir préséance sur les usages communautaires des médias.

Du côté de la télématique, l'apparition de multiples possibilités d'accès aux réseaux d'échanges pose des problèmes nouveaux en termes de préservation de la liberté d'expression en même temps que de protection de la vie privée: les usagers des réseaux peuvent-ils se permettre d'envoyer n'importe quel type de messages? Est-il possible par ailleurs de contrôler certains comportements criminels, tels les intrusions, l'injection à distance de virus et de vers, les fraudes et les vols, qui peuvent présenter diverses formes d'atteintes à la vie privée?

La santé

S'il est un domaine où l'information personnelle est considérée comme ultra-sensible, c'est bien celui de la santé. Or la protection de la confidentialité des dossiers médicaux est menacée par de multiples initiatives[6]. D'abord, les données circulent librement non seulement au sein d'établissements immenses, mais aussi entre administrations et jusqu'aux ministères pour fins de contrôle des coûts et d'implantation de politiques de soins. Ces gisements de données sont évidemment convoités par toute une série de gens, depuis les employeurs pour fins de tri à l'embauche ou de contrôle des coûts de santé jusqu'aux assureurs, aux établissements de crédit et aux agences de renseignements de crédit, aux écoles et

---

[6] En Ontario, une vaste enquête menée par le juge Krever en milieu hospitalier fut à l'origine de la longue discussion et de l'adoption de la loi de protection des renseignements personnels: Ontario Commission of Inquiry into the Confidentiality of Health Information (Mr. Justice Horace Krever), *Report of the Commission*, 3 vol., Toronto, Queen's Printer, 1980, 583 p., 533 p., 560 p.; *Freedom of Information and Protection of Individual Privacy Act*, S.O. 1987, c. 25.

aux chercheurs, pour ne pas mentionner la police, les services d'espionnage de toute sorte et les diverses administrations.

Une dimension nouvelle s'est ajoutée à la manipulation des renseignements de santé: le développement de l'information génétique et des banques de données sur l'ADN. À partir de postulats souvent douteux, on cherche à obtenir de l'information génétique sur les personnes et sur les populations pour des fins d'identification policière, de prévention médicale, de sélection dans l'emploi, de détermination de l'assurabilité des personnes. Aux États-Unis, le FBI se constitue une base de données servant à la poursuite des criminels («DNA Law Enforcement Database») ou à l'analyse de la criminalité sur la base d'un typage à partir de quelques gènes, dont la scientificité est contestable. Outre que les techniques ne sont pas sûres, ces opérations conduisent à des formes de stigmatisation et de discrimination basées sur certaines caractéristiques physiques, familiales, régionales ou ethniques, qui pourraient constituer des dangers encore plus considérables si leur usage débordait dans la société civile.

L'emploi

Le secteur de l'emploi recoupe tous les autres, et nous avons déjà recensé de multiples exemples d'agression de la vie privée des employés à leur travail et à l'extérieur. Les employeurs veulent en savoir d'autant plus sur chaque salarié que les assureurs privés exigent maintenant, aux États-Unis, des primes très fortes pour protéger les employeurs contre les coûts de santé que leurs employés pourraient leur faire encourir et contre les poursuites en responsabilité civile qu'ils pourraient leur intenter. Il s'ensuit, autant au stade du recrutement qu'en cours d'emploi, un ensemble d'initiatives visant à surveiller (*monitoring*) les travailleurs et non plus seulement leur travail: demandes de références et de renseignements de crédit, enquêtes sur leur style de vie (consommation de tabac, d'alcool, de stupéfiants), sur leurs opinions, sur leurs faits et gestes hors des lieux de travail, tri génétique, tests (de consommation de drogue, psychologiques, génétiques), surveillance des employés par terminal informatique et par téléphone, à l'occasion ou sous prétexte de contrôle de la productivité, interventions de santé (examens médicaux et banques de données intégrées).

Les usages secondaires

Signalons en outre la tendance dans tous les secteurs, et spécialement chez les usagers qui recourent à des intermédiaires de courtage d'information, à faire servir les renseignements personnels à des usages secondaires imprévus au moment de leur collecte. Ce phénomène est particulièrement inquiétant dans les domaines commerciaux du crédit et du marketing, où l'on vend et utilise de tout, particulièrement des renseignements qui accompagnent des transactions ordinaires, comme les achats par cartes de crédit. Les diverses techniques de couplages de

banques de données informatisées et de mise en réseaux de telles banques, en s'appuyant sur des identifiants quasi universels, permettent désormais de réaliser de véritables "doubles informatiques" des individus décrivant une série de caractéristiques avec une précision beaucoup plus grande que ce que la mémoire de ces personnes peut leur rappeler d'elles-mêmes.

Les problèmes internationaux

Enfin, ces problèmes se trouvent amplifiés sur le plan international par l'effet des transferts de technologies aux divers pays et par l'établissement de réseaux de communications de renseignements personnels dans ces pays et à travers le monde, pour des fins de police ou d'échanges d'informations entre agences gouvernementales (pouvant donner lieu, comme en Australie, à de vastes systèmes de corruption de fonctionnaires). On assiste de plus en plus à la constitution de fichiers de population, grâce à des opérations englobantes de recensement (Thaïlande), d'établissement de cartes d'identité (Australie, Philippines), de cartes de santé et de bénéfices sociaux (Québec, Nouvelle-Zélande), de systèmes intégrés (par exemple, entre pharmacies au Québec ou en Australie). On aura vite compris qu'avec les télécommunications toutes ces banques de données peuvent être consultées à distance et permettre de suivre les individus à la trace partout dans le monde[7].

1.2 Surveillance généralisée et contrôle social

Il est bien évident que, sur le plan individuel, les diverses atteintes à la vie privée et à l'intimité, dont nous n'avons touché ici que celles qui concernent plus particulièrement l'informatisation, sont de nature à fragiliser les personnes et à leur causer des torts précis. Mais au-delà de cette dimension individuelle, des phénomènes sociaux se font jour, dont le plus important est sans doute la mise en place d'une «société de surveillance», dans laquelle le quadrillage des populations, l'accumulation de renseignements de toutes sortes sur elles, et la diffusion tous azimuts de ces informations, nous plongent dans un type de société où nos moindres gestes ou transactions sont épiés, enregistrés et rendus accessibles au

---

[7] Pour une étude détaillée des flux transfrontières de renseignements personnels sur les Canadiens, consulter R. Laperrière, R. Côté, G. A. LeBel, P. Roy et K. Benyekhlef, *Vie privée sans frontières: Les flux transfrontières de renseignements personnels en provenance du Canada,* ministère de la Justice du Canada, 1991, 357 p.; sur les aspects juridiques de ces flux, voir R. Laperrière, R. Côté, G. A. LeBel, "The Transborder Flow of Personal Data from Canada: International and Comparative Law Issues", *Jurimetrics Journal of Law, Science and Technology*, vol. 32, 1992, p. 547-569.

monde entier et particulièrement aux organisations qui ont les moyens d'analyser ces masses de renseignements[8].

Les conséquences politiques et sociales de ce système de surveillance sont profondes: méfiance généralisée, perte d'autonomie face au contrôle des renseignements circulant sur soi, conviction qu'on ne peut plus rien cacher au gouvernement, à l'assureur ou au banquier, impossibilité de faire corriger des erreurs qui se répandent dans les systèmes interreliés, crainte que la connaissance par autrui de nos habitudes de vie et de nos opinions, révélées par nos diverses transactions, donne lieu à encore plus de discrimination à notre égard... La surveillance généralisée tend à asservir l'individu aux pouvoirs dominants et à paralyser son action politique.

Cela nous conduit plus largement, au-delà de la prophylaxie sociale installée par la surveillance, à la mise en place de contrôles sociaux, qui permettent grâce à des techniques de profilage, d'identification et de suggestion publicitaire ou autre, de modeler les comportements des consommateurs, des usagers, des bénéficiaires, dans le sens des attentes des décideurs. Des populations entières sont ainsi typées, analysées, sollicitées et pressurées par les techniques les plus raffinées du marketing et par des campagnes ciblées, pour réagir positivement aux conditionnements qui les entraînent à agir de la façon voulue[9]. On n'est plus dans *1984*, mais dans *le meilleur des mondes*, où la séduction remplace la contrainte, et où les pressions les plus efficaces sont culturelles et idéologiques. On voit ici toute l'importance de l'informatique, dont la fonction principale est le traitement et la manipulation de l'information.

1.3 L'informatique juridique

Le domaine du droit, et particulièrement de la pratique du droit, n'échappe pas à ces développements. Si la bureautique juridique n'a pas encore tenu ses promesses en termes de diminution des coûts des services juridiques pour la population, la constitution de banques de données juridiques et judiciaires entraîne de son côté un élargissement considérable des possibilités de repérage et d'analyse du droit. Nous sommes alors confrontés à la fois au problème inévitable de l'accroissement des coûts pour le justiciable, mais aussi à celui de l'aggravation des inégalités devant la justice résultant des différences de moyens.

---

[8] Ce phénomène a été mis en lumière par D. H. Flaherty, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States*, Chapel Hill, U. of North Carolina Press, 1989, 483 p. Pour un portrait saisissant de la surveillance étatique au moyen de l'informatique au Québec, voir la série d'articles de Michel Venne, "L'État sait tout", *Le Devoir,* 8-12 février 1993.

[9] Sur cette problématique, voir K.G. Wilson, *Technologies of Control: The New Interactive Media for the Home,* London, U. of Wisconsin Press, 1988, 180 p.

Par ailleurs, la modification subtile du droit par son traitement informatisé peut résulter des modèles retenus et des choix effectués à divers niveaux. Il ne peut y avoir en effet de traitement absolument neutre de l'information, et il faut se garder que l'informatisation généralisée des textes juridiques entraîne des distorsions telles l'extraction du contexte historique, la perte de vue de la hiérarchie des normes, l'aggravation de l'isolement du juridique par rapport à son contexte social, la préférence accordée à l'interprétation littérale au détriment de la recherche de l'objectif de la loi, la réification du droit comme technique plutôt que comme moyen de réaliser ou rechercher la justice.

Les systèmes experts en droit en sont à leurs premiers balbutiements: les rares expériences ne concernent que des domaines très restreints du droit, et sont réalisés dans le cadre d'opérations très précises. Contrairement à ce qu'on avait pu croire au début, le droit ne se laisse pas facilement simplifier en formules ou en règles univoques, et l'informatique ne peut fournir aux usagers des systèmes de décision automatique ou même des guides infaillibles d'application du droit aux faits. Si la tendance actuelle est de penser plutôt en termes de systèmes complexes d'information ou d'aide à la décision, l'influence éventuelle de ces systèmes sur la qualité de la décision juridique ou judiciaire, la pertinence sociale de leur intentionnalité générale et l'accès inégal à ce type de ressource restent encore à être évalués[10].

2 Les solutions envisagées et expérimentées

Pour tenter de répondre à l'ensemble des problèmes que nous avons évoqués plus haut, les pays occidentaux les plus industrialisés ont eu le réflexe premier d'établir des normes juridiques de protection des droits en légiférant. Mais on s'est vite rendu compte des limites des lois, autant dans leur formulation que dans leur application, et les pouvoirs publics ont voulu encourager les solutions contractuelles et même des initiatives non juridiques, surtout dans le secteur privé.

---

10 Voir sur l'informatique juridique, D. Bourcier et P. Mackay (dir.), *Lire le droit: langue, texte, cognition,* coll. Droit et société, vol. 3, Paris, L.G.D.J., 1992; C. Thomasset, R. Côté et D. Bourcier (dir.), *Le droit saisi par l'ordinateur; les sciences du texte juridique,* Cowansville, Yvon Blais, 1993, 472 p.

2.1 Mesures législatives

Les secteurs publics québécois et canadien

Le Québec a été la première province canadienne à adopter sa loi de protection des renseignements personnels[11], la même année que le Parlement fédéral[12], en 1982. Bien que ces lois ne mentionnent pas spécifiquement l'informatique, il est généralement admis que les progrès dans ce domaine ont été déterminants pour l'adoption de ces législations[13]. Essentiellement, elles visent à répondre à deux problèmes de façon intégrée: permettre l'accès le plus large aux documents des organismes publics, tout en protégeant la confidentialité des renseignements personnels détenus par l'administration. Ces deux grands principes sont assortis l'un et l'autre d'exceptions ou d'exemptions très larges et très nombreuses, qui en rendent l'application relativement inoffensive: on a pu remarquer que ces lois n'ont pas sérieusement empêché les gouvernements et les administrations d'accumuler et de s'échanger des renseignements personnels, et que les documents qu'ils veulent garder secrets sont toujours aussi jalousement gardés. Sans doute les lois ont rendu les administrateurs plus prudents et ont réprimé certains abus du secret administratif et du viol de la confidentialité; mais la police, les services secrets, les gouvernements et les services stratégiques des organismes publics (sécurité, contentieux, relations de travail, recouvrement de créances, etc.) n'ont pas sérieusement été touchés[14].

---

[11] *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1.

[12] *Loi sur l'accès à l'information*, S.C., 1980-81-82, c. 111, art. 2 (Annexe 1), L.R.C. 1985, c. A-1; *Loi sur la protection des renseignements personnels,* S.C., 1980-81-82, c. 111, art. 2 (Annexe 2), L.R.C. 1985, c. P-21.

[13] Les grandes enquêtes qui ont préparé la voie à l'adoption des lois canadienne et québecoise sont: Canada, ministère des Communications et ministère de la Justice, Groupe d'étude sur l'ordinateur et la vie privée, *L'ordinateur et la vie privée*, Ottawa, Information Canada, 1972; Québec, Commission d'étude sur l'accès du citoyen à l'information gouvernementale et sur la protection des renseignements personnels, *Information et liberté: Rapport de la Commission,* 1981.

[14] Sur le renseignement policier au Canada, voir S.A. Cohen, *Invasion of Privacy: Police and Electronic Surveillance in Canada*, Toronto, Carswell, 1983; et D.H. Flaherty, "Protecting Privacy in Police Information Systems: Data Protection in the CPIC", *University of Toronto Law Journal*, vol. 36, 1986, p. 116-148. La *Loi sur le service canadien du renseignement de sécurité*, S.C. 1984, c. 21, comprend des dispositions qui permettent à ce service secret de pénétrer dans presque toutes les banques de données au Canada.

Les commissaires et commissions d'accès à l'information et de protection des renseignements personnels

Une originalité canadienne dans le contexte nord-américain a consisté à instituer à Ottawa des commissaires à l'accès et à la protection des renseignements personnels, fusionnés au Québec en une seule commission d'accès à l'information. Alors que les commissaires fédéraux ne disposent que de pouvoirs d'enquête, de recommandation et d'institution de poursuites devant les tribunaux, la commission québécoise possède un pouvoir décisionnel de révision des refus d'accès de l'administration, en plus de ses pouvoirs de recommandation et d'application de la loi. Mais le bilan comparé de l'action de cette commission et de ces commissaires reste à faire.

Les secteurs publics aux États-Unis

Comme il arrive souvent au Canada, l'adoption de ces lois visant les secteurs publics n'a pas résulté d'une génération spontanée, mais est tributaire de la situation aux États-Unis, et dans une moindre mesure des influences européennes[15]. La Suède et la République fédérale d'Allemagne avaient en effet pris les devants au début des années 1970, suivies par la France en 1978 et la Grande-Bretagne en 1984[16]. Mais c'est aux États-Unis que nos législateurs sont allés chercher leur inspiration majeure. Le Congrès américain avait adopté en 1974 son *Privacy Act of 1974* [17], complété par le *Public Information Act: Agency Rules, Opinions, Orders, Records and Proceedings* [18], qui s'appliquent au niveau fédéral; pour choisir un modèle récent de législation étatique, on peut citer le *Personal Privacy Protection Law* et le *Freedom of Information Law* [19] de l'État de New York.

---

15 Pour une description et un bilan de ces lois, voir P. Péladeau et R. Laperrière, *Le droit sur la protection des renseignements personnels: étude sur les bases privées de données à caractère personnel en droit canadien, comparé et international*, Montréal, SOQUIJ, 1986, 456 p.

16 Voir en Suède, la *Loi sur l'informatique* du 11 mai 1973, amendée le 1er juillet 1984; en République fédérale allemande, la *Loi fédérale de protection des données* de 1976, amendée en 1986; en France, la *Loi relative à l'informatique, aux fichiers et aux libertés*, no 78-17 du 6 janvier 1978; et en Grande-Bretagne, le *Data Protection Act*, 1984, c. 35.

17 5 U.S.C. 552a.

18 5 U.S.C. 552.

19 Voir R.E. Smith (dir.), *Compilation of State and Federal Privacy Laws* (mise à jour périodique).

La diversité législative américaine

Le réflexe américain étant d'adopter une loi chaque fois que se pose un problème particulier, un nombre considérable de législations viennent tenter de protéger les renseignements personnels dans autant de secteurs ou pour autant de catégories de renseignements. Nous ne citerons que quelques-unes des plus importantes ou des plus récentes: l'*Electronic Communications Privacy Act of 1986,* le *Computer Fraud and Abuse Act,* les amendements actuellement discutés au *Fair Credit Reporting Act of 1970*, le projet de *Privacy for Consumers and Workers Act* (HR 1218, Sen. 516), le projet de *Computer Security Act* (Bill 266). Les spécialistes américains sont obligés de constater que les multiples lois adoptées n'ont pas arrêté la collecte et la diffusion à grande échelle des renseignements personnels; mais leur bilan est d'autant plus négatif que les lois sont très faiblement appliquées en raison de l'absence d'organisme administratif spécialisé chargé de leur mise en œuvre. En 1974, les propositions de mise sur pied d'un Data Protection Board avaient été rejetées par le Congrès, et les tentatives ultérieures de l'introduire se sont soldées par des échecs.

Le contexte international

Sur le plan international, diverses initiatives sont venues s'inscrire dans ce mouvement législatif et l'amplifier[20]. Signalons l'adoption en 1981 par le Conseil de l'Europe, de la *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel,* et la discussion actuelle au niveau du Conseil des communautés économiques européennes d'une *Proposition de directive du Conseil relative à la protection des personnes à l'égard du traitement des données à caractère personnel* [21], qui, si elle était adoptée, imposerait des normes européennes de protection des renseignements personnels à tous les membres du marché commun. Quant au Canada, il a adhéré en 1984 à la *Recommandation de 1980 concernant les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de* l'OCDE. Ces lignes directrices n'ont pas force de loi: elles visent essentiellement à favoriser la libre circulation des données entre pays occidentaux industrialisés, tout en incitant les entreprises privées à adopter des codes de conduite volontaires ou autres formes d'autoréglementation. De l'avis des spécialistes, les encouragements du gouvernement canadien aux entreprises privées d'ici n'ont pas produit de résultat sérieux pour protéger les droits des personnes.

---

[20] Pour un bilan de ce mouvement, voir un article remarqué de l'ancien commissaire à la protection des renseignements personnels du Land de Hesse, Spiros Simitis, "Reviewing Privacy in an Information Society", *University of Pennsylvania Law Review*, vol. 135, 1987, p. 707-746.

[21] Version reformulée le 15 octobre 1992.

Le secteur privé au Québec et au Canada

Pour pallier l'absence quasi totale de réglementation visant le secteur privé au Québec et au Canada, quelques lois ont été adoptées et des projets de réglementation sont actuellement en discussion. D'abord, le nouveau *Code civil du Québec*[22], qui doit entrer en vigueur en 1994, comprend un chapitre sur la protection de la réputation et de la vie privée. Ces dispositions font écho aux grands principes protecteurs des articles 4 et 5 de la *Charte des droits et libertés de la personne*[23] du Québec, et elles sont maintenant complétées par une *Loi sur la protection des renseignements personnels dans le secteur privé*[24], adoptée en juin 1993 et qui entrera en vigueur le 1er janvier 1994. Cette loi d'application générale au secteur privé est unique en Amérique; elle reprend la logique des dispositions de protection des renseignements personnels du secteur public, avec sensiblement les mêmes principes et les mêmes exceptions, et elle sera mise en œuvre par la même commission d'accès à l'information. On ne se surprendra pas qu'elle s'expose à la même critique qui vise les législations sur le secteur public, car essentiellement cette loi entend gérer l'accumulation et la diffusion des renseignements personnels plutôt que les réduire ou les contrôler. Seuls les abus les plus criants pourront être réprimés, dans la mesure où la Commission reçoit les ressources nécessaires pour s'acquitter de ce nouveau mandat et à condition qu'elle trouve la volonté politique de prendre l'initiative dans la défense et la promotion des droits des personnes fichées.

Signalons pour compléter ce portrait de la situation canadienne l'existence au niveau fédéral de discussions pour l'adoption d'un règlement de protection des renseignements personnels détenus par les institutions financières, particulièrement les banques[25], et la publication d'un énoncé de principes du ministre des Communications concernant l'autoréglementation dans ce secteur d'activité[26].

2.2 Solutions contractuelles

Dans un domaine qui évolue aussi vite que les nouvelles technologies, il est difficile de prétendre contrôler juridiquement les comportements des agents, surtout lorsqu'on ne les connaît pas bien. C'est pourquoi certains auteurs, surtout américains, suggèrent de compléter la législation par de fortes incitations aux entreprises et aux gouvernements à accorder contractuellement des droits aux

---

22 L.Q. 1991, c. 64, art. 35 à 41.
23 L.R.Q., c. C-12.
24 L.Q. 1993, c. 17.
25 Voir Canada, Sénat, Rapport intérimaire du Comité permanent des banques et du commerce, *Règlements portant sur l'utilisation par une institution financière des renseignements fournis par ses clients,* mars 1993.
26 Voir Canada, ,ministère des Communications, *Les télécommunications et la protection de la vie privée, document de travail et principes proposés,* juin 1992.

personnes sur lesquelles elles détiennent des renseignements. Ainsi pourrait se développer un marché d'achat et de vente de droits à la vie privée, ainsi que des concepts nouveaux comme la propriété conjointe des renseignements personnels au profit des organismes ficheurs et des intéressés[27]. Le problème majeur de ces suggestions, c'est qu'elles reposent sur la bonne volonté des utilisateurs d'informatique, comme si les pressions du marché pouvaient suffire à orienter les pratiques juridiques. Mais il apparaît de plus en plus évident que la combinaison gagnante résulte de la conjugaison de lois et de règlements spécifiques aux pratiques de chaque secteur avec une variété de solutions contractuelles adaptées aux diverses activités et aux attentes de la clientèle, afin que les utilisateurs de l'informatique se sentent liés et responsables et que les personnes sur lesquelles ils détiennent des renseignements disposent de recours qui, malgré leur caractère aléatoire, seront toujours préférables aux beaux discours.

2.3 Initiatives non juridiques

Comme pour les arrangements contractuels, les législateurs peuvent se contenter d'établir un cadre juridique dans lequel les acteurs sont appelés à interagir. En l'absence de politique publique sur le sujet, ceux-ci sont laissés à eux-mêmes et prennent les initiatives que leur commandent leurs intérêts ou la conscience sociale de leurs dirigeants. C'est ainsi que certains vantent le discours de promotion du respect de la vie privée des clients comme élément susceptible de procurer aux entreprises un avantage compétitif sur le marché de leurs services. Certaines options sont aussi offertes aux individus, sous forme de possibilité de faire retirer leur nom de listes de sollicitation commerciale par exemple. Des intermédiaires, comme des compagnies américaines de télécommunications ou de renseignements sur les consommateurs, prennent l'initiative d'offrir des options techniques de retrait de la collecte automatique de renseignements, ou de vérification de l'exactitude de ces renseignements. Des experts cherchent à mettre au point et à vendre des systèmes transactionnels préservant l'anonymat des clients, en même temps que se répandent en Europe les cartes prépayées (comme celles de France-Télécom) assurant de fait cet anonymat.

Les commissaires à la protection des renseignements personnels de même que divers experts consultants, dont plusieurs comptables, font la promotion ou adoptent la pratique de la vérification informatique, qui consiste à s'assurer que les systèmes répondent aux normes de gestion établies, de la même façon qu'on le fait pour la comptabilité. L'Association canadienne des normes (ACNOR-CSA) travaille sur un projet de standards qui permettrait aux entreprises qui les respectent d'obtenir un sceau d'approbation et ainsi de donner à leur clientèle une garantie

---

[27] Voir A.F. Westin, "Ten Predictions on Consumer Privacy Issues", 11 (1) *Mobius* (1992), cité dans R. Laperrière, *Le projet de loi 68 sur la protection des renseignements personnels dans le secteur privé*, mémoire présenté à la Commission de la culture de l'Assemblée nationale, le 23 février 1993, p. 42-43.

plus sérieuse de leur respect des principes de protection de la vie privée. Toutes ces initiatives sont louables, et leur succès repose davantage sur le sens des responsabilités des dirigeants d'entreprise et des gestionnaires publics que sur la contrainte juridique. Elles auront plus de chances de succès dans la mesure où le niveau d'éducation sur les droits des personnes aura augmenté, et où les personnes concernées seront appelées, à travers les organismes volontaires de défense de leurs droits, à participer à l'élaboration et à l'application des normes et procédures propres à réaliser une protection adéquate des renseignements personnels.

3 Les enjeux socio-juridiques de l'informatisation

Les solutions juridiques, et parajuridiques, apportées aux problèmes soulevés par l'informatisation, sont partielles et aléatoires, nous venons de le voir. Elles ont tout de même le mérite d'indiquer des voies, valables ou non, et de faire apparaître une série d'enjeux sociaux qui se manifestent autant sur le terrain juridique que dans les autres domaines de l'action. À travers l'informatique, nous nous trouvons ainsi confrontés à des problèmes de définition et d'extension des protections, ainsi qu'à l'évaluation des changements sociaux induits par les nouvelles technologies de l'information et de la communication. L'informatisation pose toute la question du contrôle du changement technique par les individus, celle des possibilités et expériences de contre-pouvoirs et d'arbitrages politiques, et celle de son rapport aux libertés et aux droits humains.

3.1 Problèmes de définition et d'extension des protections

La protection de la vie privée, et par inclusion et extension celle des renseignements personnels, semble reposer essentiellement sur la valorisation de l'individualisme, sans doute en raison de ses premières manifestations tournées vers la défense de l'intimité. Que des individus désirent protéger jalousement une sphère secrète de leur pensée et de leur action, voilà une valeur légitime qui ne s'oppose pas nécessairement à la sociabilité, mais qui pourrait en être considérée comme une condition d'exercice. Sans un refuge où il peut échapper un moment aux pressions sociales, l'individu deviendrait l'esclave des idées, des passions et des modes dominantes: il ne pourrait construire cette autonomie personnelle qui lui permet d'intervenir authentiquement en société dans les sphères politique, économique et culturelle. C'est là une bonne raison pour laquelle la vie privée échappera toujours à une définition juridique précise: elle traduit l'irréductibilité de l'individu face à la société. Mais elle restera toujours en tension avec le pôle de la vie publique ou sociale en raison de la nécessité des échanges sociaux, qu'ils soient ou non contrôlé, par le droit. Ainsi, l'opposition entre vie privée et vie publique

est une vue de l'esprit partielle et dichotomique: ce sont là les deux pôles complémentaires de la vie sociale[28].

Les rapports des individus à l'État sont bien souvent des rapports obligés: pour mettre en œuvre ses lois et dispenser ses services, l'État exige des citoyens le dévoilement d'un nombre considérable de renseignements personnels, touchant tout autant l'état civil et les appartenances que les biens et les revenus, l'emploi, la santé, la solvabilité, les incidents judiciaires... On devine la convoitise que suscitent les banques de données constituées à partir de déclarations des citoyens chez les organismes publics et les entreprises privées qui voudraient les faire servir à des fins différentes de celles pour lesquelles elles ont été crées.

Les corporations aussi ont des rapports obligés à l'État, et doivent divulguer un grand nombre de renseignements à diverses administrations. Mais on leur étend abusivement, à notre avis, les protections dues aux renseignements personnels et le concept même de "vie privée", qui devrait être réservé aux individus. Il en est de même pour la liberté d'expression, principe de droit rattaché à l'exercice de la citoyenneté, qu'on a indûment étendu à la "liberté d'expression commerciale". Pour l'instant, les corporations ne peuvent bénéficier des dispositions canadiennes ou québécoises de protection des renseignements personnels; mais les renseignements de nature économique qu'elles transmettent aux gouvernements font l'objet d'un droit d'accès conditionnel (et souvent discrétionnaire). Là aussi, les frontières entre ce qui est public et ce qui est privé sont difficiles à tracer.

Quant aux rapports entre les individus et les corporations, nous les qualifierions de semi-obligés. En principe, nul n'est forcé de faire affaire avec les corporations privées; mais en pratique celles-ci contrôlent une bonne partie du marché de la demande d'emploi, de sorte qu'une grande partie de la population est forcée d'y recourir pour assurer sa survie. Le secteur privé a aussi la haute main sur un vaste éventail de services essentiels dont la population a besoin: par exemple, les services bancaires et les assurances. Or actuellement, on est en situation d'absence quasi totale de protection réglementaire, contractuelle ou même volontaire des renseignements personnels détenus par le secteur privé. La nouvelle loi québécoise de protection des renseignements personnels dans le secteur privé, à l'instar des autres lois régissant le secteur public, érige le consentement des personnes en norme absolue: dès que celui-ci est obtenu, la corporation peut utiliser les renseignements selon les termes du consentement. Or ces formules de consentement sont rédigées en termes généraux qui donnent aux corporations une très large marge de manœuvre. Cette application du principe juridique du consensualisme peut jouer systématiquement contre les intérêts de la population:

---

28 Pour une étude extensive de la notion juridique de vie privée, voir F. Rigaux, *La protection de la vie privée et des autres biens de la personnalité*, Bruxelles, Bruylant, et Paris, Librairie générale de droit et de jurisprudence, 1990, 849 p. Voir aussi P. Kayser, *La protection de la vie privée*, Paris, Economica et Presses universitaires d'Aix-Marseille, 2e éd., 1990, 457 p.

et elle devrait être tempérée par l'adoption de mesures dites d'ordre public qui imposeraient des obligations précises aux détenteurs de fichiers privés.

Les rapports des individus à leurs groupes d'appartenance, qu'ils soient purement volontaires comme dans le cas des associations, ou obligatoires pour qui veut gagner sa vie comme dans le cas des corporations professionnelles et des syndicats, révèlent les mêmes conflits: la protection des renseignements personnels pèse souvent très peu en regard des bénéfices que les organisations peuvent tirer de la vente ou de l'échange des listes de noms de leurs membres, sans compter les dangers de discrimination que présente la divulgation de renseignements sur des caractéristiques particulièrement sensibles des individus concernés.

Si certains types de renseignements sont qualifiés de sensibles dans certains pays européens, et sont à ce titre beaucoup mieux protégés qu'en Amérique du Nord, c'est sans doute en raison des distinctions de culture politique et juridique, qui définissent des rapports différents à l'État, aux corporations, aux associations, à la politique, au syndicalisme, et de façon plus générale à l'autorité et à la structure sociale. L'interventionnisme étatique européen s'explique non seulement par les tristes cas anciens et récents de fichage des citoyens (par des polices secrètes comme la Gestapo et la Stasi, par exemple), mais aussi plus largement par la culture politique et administrative de ces pays. Le Québec se situe en quelque sorte à la croisée des influences européennes, par l'importance institutionnelle et l'autorité formelle données à sa commission d'accès à l'information, et des influences nord-américaines, par l'empirisme de ses normes, les multiples exceptions et limitations auxquelles leur application est assujettie, et la soumission de la solution de certaines questions aux aléas de la politique plutôt qu'à la norme juridique.

3.2 Les changements sociaux induits par les NTIC

Le développement des nouvelles technologies de l'information et de la communication (NTIC) produit une série de changements sociaux, comme nous l'avons vu à propos de leurs effets sur la vie privée qui se répercutent non seulement sur les individus mais aussi sur le type de société qu'elles induisent: une société de gestion plus rationnelle sans doute, et plus rentable économiquement pour les utilisateurs de ces technologies, mais aussi une société de surveillance et de contrôle social accrus, d'aggravation des inégalités devant la loi, et de médiation plus prononcée des rapports sociaux par la technique[29].

---

[29] Sur ces dimensions, voir D. Burnham, *The Rise of the Computer State: A Chilling Account of the Computer's Threat to Society,* New York, Vintage Books, 1984; Collectif, "L'informatisation, mutation technique, changement de société", *Sociologie et sociétés,* PUM, avril 1984; C.C. Gotlieb et A. Borodin, *Social Issues in Computing*, N.Y., Academic Press, 1973, 284 p.; J. Martin et A. Norman, *The Computerized*

À cet égard, les moyens gigantesques d'accumulation, de diffusion et de traitement de l'information personnelle ou autre ouvrent de nouvelles possibilités d'analyse des réalités sociales, et fournissent en même temps de multiples occasions de pression et de manipulation de la consommation et de l'opinion, comme on peut le constater en matière de sollicitation commerciale (marketing) et de sondages. Les dangers de concentration excessive de pouvoir, particulièrement lorsque les prises de décisions peuvent avoir des répercussions sociales considérables, vont de pair avec l'apparition de nouveaux risques d'erreurs et d'indiscrétions à grande échelle, dans des systèmes informatisés et des réseaux intégrés contre lesquels le simple citoyen est convaincu de son impuissance à obtenir des redressements aux préjudices qui lui sont causés[30].

Ces nouveaux instruments de pouvoir donnent évidemment aux décideurs la possibilité d'instituer des mécanismes de gestion sociale par profils, où les individus sont fondus dans des ensembles et des catégories sur lesquels s'exercent les actes d'autorité ou de séduction. Ils permettent aussi un contrôle des masses et de leurs comportements collectifs lorsque les ensembles considérés sont des populations entières. Mais au-delà de l'extension et du raffinement de ces actes de pouvoir, des transformations plus fondamentales ont lieu. La collecte de renseignements de toutes sortes auprès des citoyens est devenue banalisée, et elle est souvent invisible: le simple fait de donner un numéro d'identification, ou même notre nom, peut permettre à nos interlocuteurs d'avoir accès instantanément à des quantités phénoménales de détails sur notre vie personnelle, la plupart du temps à notre insu. Nous sommes devenus transparents, alors que les pouvoirs bien souvent s'opacifient; et nous sommes soumis à une inquisition beaucoup plus importante que ne le laisseraient croire les appareils ou formulaires de collecte des données.

Mais il y a plus: étant donné les possibilités de traitement de l'information offertes par l'informatique et les télécommunications, toute information prend de la valeur sur le marché: cette marchandisation de l'information donne naissance à une chasse gigantesque aux renseignements pour pouvoir les revendre ou les échanger, et la constitution de marchés noirs de l'information personnelle, souvent alimentés par une corruption systématique de fonctionnaires[31]. En raison du caractère abstrait et général de la marchandise, l'information perd sa finalité spécifique, qui en rend la collecte légitime, pour devenir un objet de commerce incontrôlable.

Ces multiples changements sociaux induisent en retour une transformation des réalités personnelles. La formalisation informatique opère une réduction de la

---

Society, Pelican, 1973, 608 p.; S. Nora et A. Minc, *L'informatisation de la société*, Paris, La documentation française, 1978, 162 p.

30 La plus fine analyse de ces dimensions politiques a été réalisée par André Vitalis, *Informatique, pouvoir et libertés*, Paris, Economica, 2e éd.,1988, 218 p.

31 À cet égard, voir les révélations d'un journaliste de *Business Week*, Jeffrey Rothfeder, dans *Privacy for Sale*, Simon and Schuster, 1992.

réalité sociale (par la modélisation qu'elle exige) et personnelle (par les applications auxquelles elle donne lieu). N'entrent en considération que les éléments formalisables et catégorisables, la plupart du temps hors contexte. Les faits retenus, dits objectifs, sont ceux dont la considération importe aux décideurs, et non ceux qui permettent d'expliquer les comportements des personnes visées[32]. Cette réduction systématique, couplée aux multiples possibilités d'erreurs et d'omissions, porte atteinte à notre sens de l'identité personnelle (nous sommes traités comme le portrait robot qu'on nous oppose) et à notre sociabilité (que pouvons-nous contre les décisions techniques centralisées?). On finit par nous faire croire en l'objectivité absolue et incontestable des systèmes techniques, qui par leur impersonnalité même devraient toujours avoir raison contre les individus cherchant à défendre leurs intérêts mesquins et à déformer la vérité en leur faveur.

3.3 Les possibilités de contrôle du changement technique

L'action des individus

Est-il possible aux personnes concernées par les changements technologiques dans les domaines de l'information et de la communication, d'exercer un certain contrôle sur ces changements ou leurs effets? Tout dépend évidemment de la position des individus dans les rapports sociaux: mais pour la majorité les possibilités d'influer sur le cours des choses, surtout lorsque des considérations techniques entrent en jeu, paraissent bien minces. Pourtant, certains textes juridiques, et surtout certaines tendances de la doctrine juridique, reposent sur les principes de l'auto-détermination informationnelle, ou plus généralement du libre choix des individus, du consensualisme (fondement du libéralisme) par opposition à la contrainte. Si tous les citoyens sont en principe égaux devant la loi, ils n'ont certes pas les mêmes moyens de défendre et réaliser cette égalité formelle. Même les diverses associations de citoyens, autant dans les domaines de la consommation que du syndicalisme ou de la défense des droits et libertés, disposent de moyens d'enquête et d'opposition rudimentaires comparés à ceux des possesseurs des systèmes techniques auxquels ils sont confrontés.

Certains invoqueront l'impossibilité d'exercer un contrôle efficace sur la circulation de l'information, en raison même de l'évolution technique accélérée dans le champ des télécommunications, et de l'extension quasi universelle de ces techniques dans tous les domaines de l'activité humaine. Si l'on pense que la "société de l'information" est en train de se construire sur la "société industrielle", sinon de la remplacer, on peut croire qu'il est devenu tout aussi illusoire de

---

[32] Cette question a été admirablement traitée par deux grands savants informaticiens américains: J. Weizenbaum, *Computer Power and Human Reason: From Judgment to Calculation*, New York, W.H. Freeman, 1976; et T. Roszak, *The Cult of Information: The Folklore of Computers and the True Art of Thinking*, New York, Pantheon Books, 1986.

contrôler l'informatisation qu'on aurait pu contrôler la mécanisation ou l'industrialisation au siècle dernier: ce seraient des phénomènes sociaux globaux qui échapperaient à la maîtrise humaine. Cette vision défaitiste doit être combattue, car l'évolution technique est une création humaine soumise à des choix éthiques non inéluctables[33].

Nous préférons continuer à préconiser diverses formes de contrôle des techniques de l'informatique et des télécommunications. Contrôles en aval sur le fonctionnement des systèmes: sur la circulation de l'information et sur les finalités de l'usage des renseignements; contrôles en amont, sur les décisions mêmes d'implantation des systèmes (idéal très rarement atteint et acquis dès lors très fragile). Pour l'instant, l'exercice de ces divers contrôles, qu'on peut approximativement qualifier de démocratiques, passe par les médias les corporations, les gouvernements, les regroupements de citoyens, et plus spécifiquement les experts de ces domaines qui de part et d'autre ont acquis une connaissance intime de ces systèmes et de leurs ramifications, et qui ont la volonté de faire servir leur savoir à un meilleur contrôle social des technologies.

Les possibilités de contre-pouvoirs et d'arbitrages

Sur le plan organisationnel et politique, comment modifier le cours des changements technologiques? Certains estiment que le marché effectue tout seul les arbitrages nécessaires: les individus rationnels arriveraient par leurs choix économiques à orienter les usages de la propriété privée dans le sens de leurs intérêts et de leurs attentes, qui réaliseraient d'eux-mêmes les équilibres souhaités. C'est ainsi que certains auteurs américains rêvent du jour où les entreprises solliciteront la permission des personnes pour utiliser leur nom et les renseignements qui les concernent.

Pour d'autres, l'action défensive et la promotion des droits des personnes passe par la vie associative: à preuve, l'intervention des groupes de consommateurs, de bénéficiaires, de défense des droits et libertés, autant devant les instances politiques qu'auprès des médias et directement dans les consultations offertes aux individus. Il ne faut pas se cacher que les chevilles ouvrières de ces actions sont souvent des gens qui ont acquis une connaissance intime du domaine, et qui consultent abondamment d'autres experts épris des mêmes idéaux. Mais une des difficultés majeures dans ce genre d'entreprise est de trouver et de maintenir des sources d'information sûres, parce que les développeurs de nouvelles technologies et les décideurs qui les implantent ont tendance à garder jalousement et jusqu'à la

---

[33] Sur les rapports entre l'informatique et l'éthique, voir R. Laperrière, "L'informatique en quête d'éthique", dans *L'éthique professionnelle, Réalités du présent et perspective d'avenir au Québec,* Cahiers de recherche éthique 13, Fides, 1989, p. 129-142. Voir aussi, plus largement, J. Nef, J. Vanderkop, H. Wiseman (dir.), *Ethics and Technology*, Wall & Thompson, 1989.

dernière minute le secret des changements qu'ils veulent mettre en œuvre, précisément parce qu'ils sont susceptibles de provoquer des bouleversements dans l'organisation du travail et le volume de l'emploi, ainsi que dans les habitudes des consommateurs et des usagers.

Peut-on compter sur nos gouvernements pour infléchir le cours du changement technologique induit par les grandes corporations et répercuté dans l'ensemble de la société? Généralement, les gouvernements sont en position de réaction et ne veulent envisager l'action que sous la pression de groupes d'intérêts. Des lois pourront être votées, mais leur application relève d'une volonté politique d'autant plus exigeante qu'elle s'applique à du long terme. Les problèmes de l'informatisation que nous avons évoqués plus haut se manifestent rarement sous la forme de cas exemplaires d'inéquité: leur dimension sociale reste invisible et leur solution n'apporte pas nécessairement de votes. Il faut penser aussi que les gouvernements sont de grands utilisateurs non seulement des équipements informatiques et télécommunicationnels, mais aussi des produits, des banques de données et des sources privées, à toutes sortes de fins, particulièrement de police et de recouvrement de créances.

Ceci dit, on doit constater chez nous comme dans de nombreux pays que l'action des fonctionnaires et de certains décideurs dans les organismes publics contribue largement à maintenir une vision critique de l'informatisation et à orienter l'activité gouvernementale vers un plus grand respect des individus et un meilleur contrôle du développement technique. La conviction est largement répandue dans ces milieux que les changements techniques enraînent des transformations sociales fondamentales et qu'il y a lieu de tenter de les maîtriser: et cette conviction finit par atteindre les milieux politiques, mais à des degrés inégaux. C'est la raison pour laquelle il est si difficile, par exemple, de tenter d'expliquer l'émergence d'une volonté politique de légiférer pour protéger les renseignements personnels dans le secteur privé au Québec, ainsi que les divers arbitrages qui ont conduit à l'adoption du texte de loi tel qu'il se présente dans sa version définitive[34].

L'importance accordée aux problèmes de protection des droits des personnes dans un contexte d'informatisation s'est aussi traduite par la création d'organismes spécialisés de surveillance du gouvernement: les commissaires et commissions de protection des renseignements personnels. Au Québec particulièrement, la Commission d'accès à l'information est dotée de pouvoirs décisionnels pour faire appliquer une loi qui a préséance sur toutes les autres lois. De ce fait, elle est en

---

[34] *Loi sur la protection des renseignements personnels dans le secteur privé*, L.Q. 1993, c. 17 ("projet de loi 68", sanctionnée le 15 juin 1993, en vigueur probablement à compter du 1er janvier 1994, voir art. 115). Pour une analyse critique détaillée de cette loi, voir Groupe de recherche informatique et droit, R. Laperrière, *Le projet de loi 68 sur la protection des renseignements personnels dans le secteur privé*, mémoire présenté à la Commission de la culture de l'Assemblée nationale, le 23 février 1993, 82 p.

position de censeur de l'action gouvernementale et de celle des organismes publics et parapublics, dans le domaine particulier de la protection des renseignements personnels[35]. Mais elle doit aussi conseiller le gouvernement et les organismes dans leur gestion de l'information. Ce double mandat est délicat à remplir[36], d'autant plus que l'intégration de la commission de surveillance à la culture de la fonction publique et le caractère politique du poste de président de la Commission peuvent faire perdre de vue à celle-ci les intérêts et les besoins de la population en général. Apparaît alors la nécessité de développer à long terme une vision du phénomène de l'informatisation sociale accompagnée d'une volonté politico-administrative de l'infléchir dans le sens de la réalisation des idéaux inscrits dans la loi et de modeler l'action décisionnelle en conséquence. Tâche considérable s'il en est pour un organisme public, et qui mériterait de faire l'objet d'évaluations indépendantes, la Commission d'accès à l'information ayant été la seule au Québec jusqu'à maintenant à avoir proposé des bilans de son action[37].

Quant aux tribunaux, leur influence dans la maîtrise des progrès informatiques s'est fait sentir surtout au niveau de la protection de la propriété, en raison de la

---

35 Pour une analyse comparée du rôle de ces commissions, voir A. Vitalis et R. Laperrière, "La démocratie assistée par des sages: l'exemple du contrôle de l'informatisation", dans J. Lamoureux (dir.) *Droits, liberté, démocratie*, Les cahiers scientifiques, no 75, ACFAS, 1991, p. 187-202.

36 Ce double mandat avait été critiqué dès 1991 par le Groupe de recherche informatique et droit dans R. Laperrière, *La protection juridique des renseignements personnels dans le secteur privé québécois*, mémoire présenté à la Commission des institutions de l'Assemblée nationale, le 13 novembre 1991. L'argument a été repris dans une contestation que l'Hydro-Québec vient de lancer en cour supérieure contre une ordonnance de la Commission d'accès à l'information, la société d'État soutenant que ces multiples mandats contreviennent à la Charte des droits et libertés de la personne. Voir M. Venne, "Hydro-Québec attaque en cour le chien de garde de la vie privée", *Le Devoir*, 22 septembre 1993.

37 Québec, Commission d'accès à l'information, *Une vie privée mieux respectée, un citoyen mieux informé: Rapport sur la mise en œuvre de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, 1987, 196 p.; Québec, Commission d'accès à l'information, *Un passé éloquent, un avenir à protéger: Rapport sur la mise en œuvre de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, 1992, 49 p. En matière de bilans d'organismes, ceux de la Commission nationale informatique et libertés (CNIL-France) méritent d'être cités en exemple en raison de leur valeur analytique, de leur détachement et de leur largeur de vue: Commission nationale de l'informatique et des libertés, *Dix ans d'informatique et libertés*, Paris, Economica, 1990, 256 p.; Commission nationale informatique et libertés, *12e Rapport d'activités*, 1991, Paris, La documentation française, 1990, 387 p. Par ailleurs, au Canada, c'est un comité parlementaire qui a été chargé d'évaluer l'action des commissaires; le rapport en a été rédigé par le professeur D.H. Flaherty et a paru sous le titre: Comité permanent de la Justice et du Solliciteur général, *Une question à deux volets: comment améliorer le droit d'accès à l'information tout en renforçant les mesures de protection des renseignements personnels*, Ottawa, Imprimeur de la reine, 1987, 150 p.

création de juridictions parallèles spécialisées dans la protection des renseignements personnels. Ces institutions ne sont pas équipées pour prendre l'initiative, mais plutôt pour résoudre des problèmes en dernier recours. Elles n'ont pas été amenées jusqu'à présent à jouer un rôle décisif dans la résolution des questions évoquées ci-dessus; et dans les pays où on leur a confié en exclusivité l'application des lois de protection des renseignements personnels, comme aux États-Unis, on déplore l'absence d'organismes publics spécialisés qui pourraient à la fois offrir des recours accessibles, élaborer une action multifonctionnelle efficace et constituer un réservoir d'expertise pour conseiller les parties plutôt que de tenter uniquement de départager leurs droits, comme les tribunaux sont réduits à le faire.

Le rapport aux libertés et aux droits humains

Cette action des individus, des groupes et des organismes n'a de sens que si l'on conçoit le progrès technique non pas comme une fin en soi, ou comme un phénomène inéluctable, mais comme une série de moyens de promouvoir des valeurs sociales supérieures permettant à tout le monde de réaliser sa destinée. Sur le plan du droit, ces valeurs sont consacrées dans des chartes de droits et libertés, et, pour ce qui nous concerne, elles s'articulent autour de deux axes principaux: les libertés individuelles et les droits sociaux. D'abord, liberté d'exister comme individu à part entière: c'est le fondement de l'inviolabilité de la personne et du principe d'égalité, c'est la liberté qui nous fait échapper à la surveillance généralisée et au contrôle social englobant, c'est celle qui se conjugue à la liberté d'autrui et qui permet de développer des rapports sociaux dépassant la simple comptabilité des droits et obligations. Intimement liée à la précédente, la liberté d'expression (et de style de vie) permet d'échapper aux conditionnements sociaux, particulièrement dans le domaine de l'information et de la communication; elle se traduit par l'irréductibilité de la personne à des caractéristiques, à des profils et à des modèles préétablis, et par l'élargissement de l'aire des choix individuels.

Mais ces libertés resteraient des coquilles vides si elles n'étaient complétées par des droits sociaux, permettant effectivement aux personnes de se réaliser en société. D'où l'importance du droit à l'éducation et à la culture, qui se traduit notamment par l'accès à l'information et aux échanges. Les supports informatiques et les réseaux de communication deviennent rapidement des passages obligés de la culture et du savoir: il faut éviter que l'érection de barrières techniques, professionnelles et financières n'en réservent le monopole aux mieux nantis. Les nouvelles technologies devraient aussi être mises à contribution pour promouvoir le droit de participation à la démocratie: la disponibilité plus grande de l'information dans le temps et dans l'espace de même que les possibilités nouvelles d'expression ouvertes par ces technologies pourront nous conduire à des formes de télédémocratie qui compléteraient harmonieusement les forums et modes d'expression actuels.

Conclusion

Nous aimerions conclure en rattachant les considérations développées dans ce texte à l'ensemble des résultats d'un vaste programme interuniversitaire de recherche sur le droit et les technologies, mené conjointement par le Centre de recherche en droit public de l'Université de Montréal et le Groupe de recherche informatique et droit de l'UQAM. Son étude des dimensions juridiques des changements technologiques, orientée vers la maîtrise sociale de ces phénomènes, a conduit à formuler six propositions sur l'émergence de leur encadrement normatif[38]:

1) Les normes se créent, émergent et se développent dans un contexte où les dimensions supranationales et multinationales des phénomènes technologiques prennent une dimension croissante, voire prépondérante *(principe d'internationalisation normative)*;
2) Les normes font appel à un nombre important de concepts flous, également appelés normes à contenu indéterminé ou variable *(principe de variation contextuelle)*;
3) L'autoréglementation constitue une part importante des phénomènes normatifs observés dans l'ensemble des champs liés aux nouvelles technologies *(principe d'autodétermination normative)*;
4) Le droit entretient des rapports d'internormativité importants avec l'éthique, dont l'importance semble s'accroître en raison des phénomènes d'incertitude croissante occasionnés par les développements technologiques *(principe de convergence du juridique et de l'éthique)*;
5) La création des normes (juridiques, éthiques ou autres) fait appel à la représentation symbolique du réel que les normes entendent organiser *(principe de représentation symbolique)*;
6) Les normes se développent dans une dialectique constante entre le privé et le public; les choix de société qu'appellent les nouvelles technologies mettent en lumière ce phénomène ancien avec une acuité nouvelle *(principe de tension entre les droits de la personne et les solidarités collectives)*.

Nous croyons avoir illustré l'application et la pertinence spécifique de ces six propositions dans le champ des technologies de l'information et de la communication. Les nouvelles technologies, et particulièrement celles de traitement et de diffusion de l'information, placent la société dans des situations inédites, non seulement sur le plan de la technique et de l'économie, mais aussi sur le plan de la justice: atteintes à la vie privée, pertes d'autonomie dans les processus décisionnels automatisés, surveillance et sélection des personnes dans les

---

38 R. Côté, P. Mackay, G. Rocher et P. Trudel, *Le programme interuniversitaire de recherche sur le droit et les technologies: bilan et perspectives. Cadre conceptuel et propositions sur l'émergence des normes dans l'univers technologique,* Cahiers du Centre de recherche en droit public et Recherches du département des sciences juridiques, 1992, p. 14.

domaines de l'emploi ou des assurances, dépendance envers les empires informationnels, érosion de la souveraineté nationale, politique, économique et culturelle. Notre préoccupation principale consiste à analyser dans quelle mesure le droit peut être mis à contribution pour résoudre les problèmes et contradictions résultant de l'accumulation, du traitement, de l'usage et de la diffusion de l'information, dans des domaines aussi cruciaux que l'emploi et le travail, la santé et la médecine, la consommation et les assurances, la police et la justice. Pour y répondre, il s'avère indispensable, comme nous avons tenté de le faire, d'élargir le cadre traditionnel d'analyse juridique pour y intégrer des éléments de pluralisme et d'évaluation sociale ainsi que des considérations particulières sur les mécanismes et les effets spécifiques des innovations technologiques.

René LAPERRIÈRE
Groupe de recherche informatique et droit
Université du Québec à Montréal

Résumé

Les nouvelles technologies de l'information et des communications posent des problèmes sociaux inédits, particulièrement en ce qui concerne la protection de la vie privée des personnes. Elles donnent naissance à une société de surveillance généralisée et ajoutent aux moyens de contrôle social. En transformant le droit et sa pratique, elles peuvent contribuer à aggraver les inégalités devant la loi. La réglementation ne suffit pas à enrayer l'accumulation et la diffusion incontrôlées des renseignements: elle doit être complétée par des arrangements contractuels et des initiatives non juridiques faisant appel à la participation des décideurs et des citoyens, et conduisant à une redéfinition des rapports sociaux entre individus, corporations et État.

Mots clés: Droit, technologie, information, informatique, communication, personne, renseignements personnels, vie privée, surveillance, contrôle social.

Summary

New information and communications technologies engender many new social problems, particularly with respect to the protection of privacy. They lead to a surveillance-society and add to the means of social control. In transforming law and legal practice, they may aggravate the inequalities before the law. Regulations are not sufficient to contain the uncontrolled accumulation and divulgation of personal information. They must be complemented by contractual arrangements and non-legal initiatives involving the participation of managers and citizen, and they should lead to a redefinition of social relations between individuals, corporations, and the state.

Key-words: Law, technology, information, computer, communication, person, personal data, privacy, surveillance, social control.

Resumen

Las nuevas tecnologías de información y comunicaciones plantean problemas sociales inéditos, particularmente en lo que concierne la protección de la vida privada de las personas. Éstas dan nacimiento a una sociedad de vigilancia generalizada y se suman a los medios de control social. Transformando el derecho y su práctica, ellas pueden contribuir a agravar las desigualdades ante la ley. La reglamentación no es suficiente para detener la acumulación y la difusión descontroladas de las informaciones: ésta debe ser completada por arreglos contractuales e iniciativas no jurídicas apelando a la participación de los decisores y de los ciudadanos, y conduciendo a una redefinición de las relaciones sociales entre los individuos, corporaciones y Estados.

Palabras claves: Derecho, tecnología, información, informática, comunicación, persona, información personal, vida privada, vigilancia, control social.