

L'émergence des sociétés de surveillance

PAR DAVID H. FLAHERTY *

Les droits de l'homme sont-ils en retard sur l'informatique et, demain, le monde occidental sera-t-il celui de la communication ou de la surveillance ? Ces questions, fondées particulièrement sur l'étude de cinq cas (Canada, France, RFA, Suède, USA), Flaherty les a posées crûment aux commissaires à la protection des données lors de leur X^e rencontre internationale à Québec et *Terminal* le remercie d'avoir bien voulu nous autoriser la publication de cet article extrait de sa conférence.

LA DÉMARCHE des futurologues manque souvent de profondeur historique, pourtant se pencher sur le passé est, à mon avis, un excellent moyen de réfléchir à l'avenir.

C'est pourquoi, historien de formation, je voudrais aujourd'hui retracer l'évolution de la protection de la vie privée et des données d'ordre personnel depuis ses origines, aux alentours de 1970¹ et examiner ce que les tendances actuelles laissent entrevoir pour l'avenir. Or, ce qui s'est passé jusqu'à présent ne m'incite guère à l'optimisme et il me semble nécessaire d'en avertir la classe politique et le grand public. Je crois que nous sommes tous de plus en plus fichés dans les banques et registres de données des secteurs privé et public ; nous devons donc réfléchir aux répercussions de ces pratiques sur la qualité de la vie dans les sociétés occidentales et aussi sur la protection des droits de la personne. De plus, en dépit des lois et des agences, j'ai bien l'impression que ladite protection n'est en fait qu'une douce illusion. S'il est possible de donner quelques exemples concrets de banques de données "menaçantes", je crois pour ma part que c'est plus la prolifération de ces banques de renseignements que l'existence de telle ou telle qui menace le droit à la vie privée, aujourd'hui et dans l'avenir immédiat. La plupart de mes exemples sont tirés de l'Amérique du Nord où, me semble-t-il, la technologie de l'information avance plus vite que la réglementation et le contrôle, notamment dans le secteur privé ; mais je sais fort bien que l'Europe n'est pas épargnée, comme le prouveront mes propos sur la Suède.

L'un des traits des sociétés industrielles occidentales, dont on néglige trop souvent de

parler, est ce risque qu'elles courent de devenir des sociétés de surveillance – si ce n'est déjà fait – en entrant dans l'ère de l'information. L'expression *société d'information* a beau être très galvaudée, elle caractérise assez bien un contexte où les échanges de renseignements se font par ordinateurs et réseaux de télécommunication.

Les bases de données informatisées actuelles permettent une surveillance intégrée de chaque citoyen au Canada et à l'étranger. Le droit qu'on nous fiche la paix est menacé, mais jusqu'à présent on n'a trouvé que des solutions partielles. C'est ainsi que la base de données du bureau de crédit de Toronto contient des renseignements de solvabilité sur dix millions d'Ontariens. Dix pour cent environ de la population adulte du Canada est fichée dans le réseau informatique de la police². Les gouvernements fédéral et provinciaux ont de très nombreuses banques de données sur divers segments de la population. Les sociétés qui émettent des cartes de crédit, American Express par exemple, ont fiché une clientèle relativement aisée dont elles peuvent, par simple vérification de carte en temps réel, connaître les allées et venues et parfois même les achats. Revenant de Paris une avocate américaine a été informée par sa banque que quelqu'un – elle-même en fait – avait acheté des vêtements avec sa carte de crédit. Elle a bien sûr très mal pris ce qu'elle percevait comme une intrusion déplacée. Les banques vous surveillent, elles aussi, grâce à la constitution de dossiers et à l'utilisation des guichets automatiques.

Dans les années 60, l'apparition des gros ordinateurs fit craindre le règne d'une mégaban-

¹. J'ai recueilli des données détaillées sur la protection des données au Canada, en Allemagne de l'Ouest, en France, en Suède, au Royaume-Uni et aux Etats-Unis.

². Voir David H. Flaherty : *Protecting privacy in police information systems : data protection in the canadian police information centre (CPIC)*, in *University of Toronto law journal* XXVI, (1986), 126.

que de données couvrant tout le pays ; ce sort a été épargné au monde occidental, mais nous nous retrouvons aujourd'hui avec une multitude de banques de données qui, bien que disséminées, ont de formidables capacités de surveillance active et passive et les coûts du stockage des données ne cessent de dégringoler. Ainsi, on peut aujourd'hui acheter l'annuaire téléphonique de toutes les grandes villes du Canada sur une simple disquette souple ; les données peuvent être compilées, enrichies, intégrées et rappelées en quelques secondes pour avoir des profils individuels. Tout le monde ne trouve pas que ces activités soient innocentes...

Panoptique électronique

L'automatisation croissante des lieux de travail permet de son côté une surveillance électronique insidieuse mais efficace de la main-d'œuvre, et notamment des sans-pouvoir de la société : personnel non syndiqué, surnuméraires, travailleurs à temps partiel, bref, les couches les plus défavorisées. C'est ainsi que les états de rendement journalier servent à surveiller le travail des préposés aux réservations des compagnies d'aviation et des opératrices qui entrent des volumes considérables de données dans ces banques dont nous parlons justement.

L'emprise croissante de la société de surveillance se manifeste également dans les multiples tentatives pour faire accepter des technologies qui empiètent sur la vie privée des citoyens, comme par exemple le polygraphe (détecteur de mensonge) et l'analyse d'urines (pour repérer les consommateurs de drogues). On pourrait également citer à cet égard le bracelet électronique, le test anti-Sida obligatoire et le dépistage génétique³. Ces initiatives illustrent fort bien la recherche d'applications des dernières découvertes si caractéristique de l'évolution récente. Ce ne sont plus les patrons qui demandent aux technocrates de résoudre tel ou tel problème ; ce sont les progrès technologiques qui incitent à trouver de nouveaux problèmes. Les inventeurs californiens d'un appareil d'analyse d'urines appelé Emit – un nom prédestiné – ont tout naturellement cherché un marché pour leur trouvaille (d'une fiabilité douteuse d'ailleurs !). Inutile de préciser que la machine avait d'abord été testée et utilisée sur des prisonniers, ce qui en dit long sur l'impuissance de certains groupes et sur le sort de gens qui doivent lutter pied à pied pour que soit respecté leur droit à la vie privée le plus élémentaire. Ces incursions dans l'intimité des citoyens, notamment de la part du secteur privé, ne sont pratiquement pas réglementées en Amérique du Nord. Huit des dix provinces du Canada n'ont aucune loi sur la protection des renseignements

pour le secteur public ; quant au secteur privé les Canadiens en sont réduits à se fier à son autodiscipline.

La Suède peut être considérée comme la société de surveillance type du monde occidental. En effet, tous les éléments y sont : automatisation poussée des renseignements sur les citoyens, numéro d'identité qui simplifie les recoupements de dossiers, circulation massive de données intégrées entre les secteurs public et privé. Le principe de transparence garanti par la célèbre loi sur la liberté de la presse permet de mettre à la disposition de chacun toutes sortes de données d'ordre personnel qui restent normalement confidentielles dans les autres pays. Par exemple, les données sur les revenus et les biens contenues dans les registres publics sont régulièrement publiées dans chaque comté ; elles ont quelques applications pratiques comme les vérifications de solvabilité mais sont aussi livrées en pâture à la curiosité du premier venu. Un fichier de la population suédoise avec nom de chaque citoyen, numéro d'identité, adresse, nationalité, statut matrimonial, revenu imposable, capital imposable et biens peut être consulté par tout un chacun.



* Historien, spécialiste des débuts de l'industrialisation. University of Western Ontario.

Ces remarques sur la Suède ne sont pas une attaque en règle contre une société qu'on peut considérer à maints égards comme un modèle de réussite ; je ne me permettrais pas de critiquer le droit des Suédois et de leurs élus à décider dans quel type de société ils veulent vivre. Pour préciser ma pensée, je dirais que tout en m'interrogeant sur les possibilités de vie privée en Suède, je ne prétends nullement que les Suédois soient moins libres que vous et moi. Ce qui me frappe dans cette société c'est le peu d'espace – physique, mental et comportemental – laissé à l'individu dans ses rapports avec l'Etat et avec ses concitoyens. La sphère du privé y est beaucoup plus réduite que dans les autres sociétés occidentales (en dehors de la Scandinavie). Je ne parle pas des aspects matériels de la vie privée, mais des éléments qui empêchent l'anonymat, l'intimité, le quant-à-soi⁴. Je crois qu'une existence équilibrée exige que l'on ait vraiment la possibilité de se retirer de temps à autre de la sphère publique afin de goûter et de cultiver son individualité.

La Suède, un paradis pour les banques de données

En Suède, rares sont les renseignements privés que l'on peut soustraire à la curiosité de ses concitoyens. En fait, les administrations en savent beaucoup plus long sur la vie des citoyens que n'importe quel fouineur ou Sherlock Holmes amateur et elles fournissent ces renseignements (qui contrairement aux données statistiques et scientifiques relèvent de la vie privée) à qui les demande, en particulier à la presse. Cet exemple montre qu'il est techniquement possible de créer une société de surveillance impeccablement efficace. Le cauchemar imaginé par Orwell ne relève plus de la science-fiction. La surveillance électronique, les réseaux de télécommunication et les bases de données relationnelles commencent seulement à influencer sur la vie privée mais ce sont des "créneaux extrêmement porteurs" !

Pour en revenir à la Suède, on y a décidé le recensement de tous les bateaux de plaisance (plus d'un million), sous prétexte que certains auraient été payés avec le produit de fraudes et d'évasions fiscales. Chacun doit payer sa juste quote-part d'impôt et personne ne doit s'engraisser sur le dos de l'Etat. Tout louable qu'il est dans une société démocratique, ce *credo* se traduit à un niveau pragmatique par la transformation de la Suède en un *paradis des banques de données* selon l'admirable formule de Jan Freese. La possibilité de créer des sociétés de surveillance devrait nous inciter à affronter la question essentielle de leur bien-fondé, mais les impératifs économiques ne nous laissent guère le temps d'examiner les valeurs humaines que nous laissons piétiner. Voulons-nous habiter dans un pays où l'économie souterraine et le système D ont été écrasés par l'embrigadement et le contrôle de l'Etat ? C'est pourtant en ces



termes que le problème se pose pour nous tous, pour nos élus et plus particulièrement pour les responsables de la protection des données.

Les choix actuels de la Suède ne sont pas le résultat d'une pondération de valeurs et d'objectifs contradictoires mais une fuite dans une multitude d'initiatives technologiques sans que soit prise en compte l'existence quotidienne de Monsieur tout-le-monde. Signe d'une résistance instinctive au côté *Big Brother* des gouvernements, des conflits et des poussées de fièvre (comme en Suède à la suite d'une proposition de recensement démographique informatisé) risquent de se multiplier, ne serait-ce que par contagion d'un pays à l'autre, puisque l'intégration de nouvelles techniques de surveillance continuera à s'accélérer dans les années 90. Et l'évolution est si rapide qu'il est à craindre d'avoir été trop optimistes sur les chances de préserver le droit à la vie privée dans les années qui viennent.

De l'efficacité des agences de protection des données...

S'il est vrai que des amorces de réglementation visent à protéger l'individu tout en évitant de créer des obstacles superflus aux avancées technologiques, la question essentielle est la suivante : les lois et les agences de protection des données peuvent-elles, dans leur état actuel, empêcher la naissance des sociétés de surveillance⁵ ? ou bien ont-elles pour fonction de faire diversion en berçant l'opinion d'un sentiment de sécurité illusoire ? De plus, le démantèlement progressif des agences de réglementation ne me

³. Voir dans le New-York Times, 22 avril 1987, page D7, la description détaillée des appareils de surveillance électronique des prisonniers en liberté conditionnelle et les efforts de promotion de ces gadgets.

⁴. Voir Alan F. Westin : Privacy and freedom (N.Y. 1967). Je remercie mes amis suédois avec qui j'ai eu en juin 1987 de fructueuses conversations qui m'ont permis d'étayer mon argumentation. Je ne les nommerai pas afin de ne pas les associer à un point de vue qui n'engage que moi.



dit rien qui vaille. Nous nous trouvons en face d'une double menace : invasion de la vie privée et affaiblissement des infrastructures de protection mises en place jusqu'à présent.

L'histoire de la réglementation démontre que, avec l'âge, les meilleurs chiens de garde perdent leur vigilance. Dans le cas des protecteurs des données, ce phénomène n'est pas le résultat d'un manque de bonne volonté, mais un processus naturel d'évolution qui touche toutes les administrations. La première loi sur la protection générale des données a été adoptée par le Land de Hesse en 1970. La Finlande a suivi le mouvement en 1987 et d'autres pays comme l'Australie et les Pays-Bas devraient l'imiter bientôt. Ce souci de protection des données est bien sûr un progrès élémentaire et indispensable. Mais il me semble que la protection, dans les pays qui se sont dotés de lois à cette fin, s'est enlisée dans la routine, dans ce qu'il nous faut bien appeler la banalisation.

Les ténors de la première génération, celle des années 70, ont quitté le devant de la scène : je pense notamment à Hans Peter Bull en Allemagne de l'Ouest et à Jan Freese en Suède. Seul Spiros Simitis reste en selle dans le Land de Hesse. Ces pionniers ont en grande partie été remplacés par de sobres fonctionnaires au style plus conforme à l'approche feutrée de la réglementation ordinaire. Pourtant la génération des années 80 compte dans ses rangs des administrateurs chevronnés et compétents et des gens qui, comme John Grace et Marcel Pépin, connaissent les médias comme leur poche. Mais la relève

risque d'être moins frondeuse car les gouvernements commencent à se fatiguer de ces interventions répétées (et nécessaires) au nom du droit à la vie privée. Enfin, bien que la protection des données ait des connotations politiques évidentes, en ce sens qu'elle met en jeu des valeurs et des intérêts contradictoires, les agences doivent se garder d'être des girouettes politiques, c'est-à-dire de modifier leurs exigences de protection en fonction des gouvernements. Cet opportunisme serait dérisoire en regard des risques actuels, d'autant plus que de son côté, la classe politique écarte allègrement toute considération de droit à la vie privée dans sa recherche de solutions aux problèmes de l'heure, toxicomanie, évasion fiscale ou atteintes à la sécurité.

Protection ou caution

Au fond, les agences de protection des données, telles qu'elles fonctionnent actuellement, servent à bien des égards à cautionner les nouvelles technologies. Leurs fonctions de consultation et de réglementation n'empêchent pas l'implantation de nouvelles technologies menaçantes (comme les cartes d'identité à lecture automatique et les innombrables banques de données hypersophistiquées) et seuls des ajustements mineurs sont obtenus. En réalité, elles n'ont guère les moyens de résister. C'est ainsi que les spécialistes de la protection des données d'Allemagne de l'Ouest ont été à peu près tenus à l'écart de la loi sur le recensement de mai 1987, puis leurs prises de position en faveur de ladite loi n'ont pas empêché les controverses et une opposition farouche. Personne ne croit plus aux grandes protestations de confidentialité. Et comment pourrait-il en être autrement quand on sait que les renseignements sur seize millions de contribuables ont été volés en novembre 86 dans le bureau torontois de Revenu Canada, une fuite que John Grace, commissaire à la protection de la vie privée, a qualifié de Tchernobyl de la protection des données ⁶.

Qui peut blâmer les citoyens de craindre la mise en réseau des banques de données quand les gens censés les protéger ne peuvent, malgré tous leurs efforts, empêcher les dérapages ? La dure réalité, c'est que les protecteurs des données risquent de devenir des francs-tireurs qui affrontent à coups de fourches et de pioches un géant bureaucratique et technocratique doté d'un arsenal nucléaire. C'est particulièrement vrai dans le secteur public où ils doivent protéger les citoyens dans leurs rapports avec un gouvernement qui se trouve être leur propre employeur. Le problème tourne essentiellement autour d'une question de pouvoir. Pour ce qui est des conflits de pouvoir internes, ce sont les administrations dont les activités sont les plus menaçantes pour la vie privée (impôt, bien-être social, police) qui répugnent le plus à ce qu'on mette le nez dans leurs affaires complexes et souvent secrètes et comme elles sont des pions essentiels sur l'échiquier budgétaire, on les écoute. En ce qui con-

⁵. Voir David H. Flaherty : Limiting governmental surveillance and promoting bureaucratic accountability : the roles of data protection agencies in western societies in *Science, technology and human values*, XI, n°1 (1986), 7-18.

⁶. Rapport annuel du commissaire à la protection de la vie privée 1986-87 (Ottawa, 1987), p. 2-3.

cerne les conflits de pouvoir *externes*, les agences de protection des données doivent tenter de comprendre les énormes enjeux des dirigeants tout en essayant, avec leurs faibles moyens, de rallier l'opinion à leurs vues. En période de vaches maigres, si l'efficacité exige qu'on empiète sur la vie privée au nom de la rationalisation et de la rentabilité, personne ne va vraiment protester, puisque l'élite est plus ou moins épargnée et que les exclus du pouvoir n'ont pratiquement aucune influence sur les prises de décision. Autrement dit, les groupes intéressés au premier chef par la protection des données, c'est-à-dire les bénéficiaires de l'aide sociale, les prisonniers et les fraudeurs de l'impôt, sont aussi les plus marginalisés. Bref, ce sont toujours les mêmes qui trinquent.

Petits mais teigneux !

Pour prendre un exemple des limites du pouvoir des agences, la louable volonté d'anti-bureaucratisme qui les a incités à avoir des effectifs peu importants pourrait en fait nuire à la protection des données. Les vérifications et les inspections sont, jusqu'à présent, notoirement insuffisantes (en dépit de progrès sensibles, en Allemagne de l'Ouest et au Canada notamment). Aussi cette rareté des interventions doit-elle être compensée par la sévérité des représailles. Les fonctionnaires qui ont accès à des renseignements personnels doivent avoir aussi peur de la vérification de confidentialité que les contribuables ont peur de la vérification de l'impôt.

Les bureaux de protection des données ont donc d'importants problèmes d'indépendance et d'autorité, leur seule chance est de trouver un appui du public, et notamment des médias. Ce qui s'est passé au Canada, en Allemagne de l'Ouest et en Suède démontre, à mon avis, que l'opinion peut se mobiliser autour de ces objectifs. La protection de la vie privée des citoyens est un combat essentiel, puisque les individus sont de plus en plus désarmés devant la révolution du traitement de l'information. La protection des données est aussi importante que la question nucléaire et la sauvegarde de l'environnement. Ceux qui en ont la charge doivent se battre pour obtenir budgets et effectifs, pousser à la réactualisation permanente des lois, dégager les moyens nécessaires aux vérifications et aux inspections, développer des contacts internationaux qui permettent de contrôler le déploiement massif des technologies de l'information, préciser les modalités des lois contre la fraude tout en évitant que le débat ne s'enlise dans des arguties juridiques.

Plus important encore, le Canada et les Etats-Unis, pour ne citer qu'eux, doivent savoir s'ils peuvent continuer à fonctionner sans loi générale de protection des données ou sans agence de protection ayant quelque autorité sur le secteur privé. L'Europe a beaucoup à nous apprendre à cet égard. Le Comité de la Justice de la Chambre des communes et un groupe de recherche du Québec ont recommandé d'importantes

initiatives judiciaires dans ce domaine⁷. La loi semble vouloir suivre le rythme de l'évolution technologique, comme l'indique le fait que le Land de Hesse, où est né le concept qui nous occupe, a adopté une loi sur la protection des données et qu'un comité parlementaire vient de proposer d'importants amendements à la loi sur la protection des renseignements personnels votée en 1982⁸.

Les protecteurs des données doivent acquérir des compétences et des connaissances toujours plus vastes sur la technologie de l'information afin de pouvoir en surveiller l'évolution (ce qui n'est pas le cas actuellement) ; ils doivent dépasser les frontières et les traditions juridiques nationales ; il est essentiel, enfin, que la loi générale sur la protection des données soit mieux ciblée, seule une législation sectorielle peut adapter les principes de la protection générale à chaque problème particulier et donc assurer aux individus des droits précis et applicables. Dans une situation idéale, comme celle créée en Allemagne de l'Ouest par la décision du tribunal constitutionnel sur le recensement de 1983 (les citoyens ont eu le droit de décider de l'utilisation des renseignements le concernant), les efforts de législation sectorielle peuvent donner un ancrage constitutionnel au droit à la vie privée. Il est cependant symptomatique du climat actuel que, même en Allemagne de l'Ouest, le respect du jugement de 1983 est loin d'être acquis.

Comment apparaîtront les organismes de protection des données en l'an 2000 ? Seront-ils considérés comme des Don Quichotte lancés contre les moulins à vent de la technologie ou comme les artisans de la coexistence pacifique de valeurs humaines et sociales contradictoires ? Je veux croire que le modèle actuel – c'est-à-dire une agence de protection des données chargée de défendre le droit permanent à la vie privée – restera très longtemps valide, en dépit des problèmes que j'ai évoqués plus haut. Je terminerai sur une note plus réconfortante en rappelant l'échec des Puritains qui ont eux aussi essayé d'imposer une société de surveillance dans la Nouvelle-Angleterre du XVII^e siècle. Lorsque j'ai commencé mes recherches sur les Puritains, j'avais l'image d'une société où tout droit à la vie privée était exclu. Les chefs puritains propageaient une idéologie familiale, religieuse et politique qui encourageait la surveillance de tous au nom d'impératifs moraux, puisque le devoir de chaque citoyen était d'aller obligatoirement au Paradis... Eh bien, sachez que les Puritains n'ont pas réussi à institutionnaliser cette surveillance généralisée car les citoyens, et au premier chef les forces de l'ordre, ont résisté à cet embrigadement et à cette mise au pas⁹. En définitive, aujourd'hui comme hier, chaque être humain veut qu'on le laisse tranquille dans son coin de temps en temps. C'est peut-être ce trait universel qui sera notre planche de salut face aux attaques réitérées contre le droit à la vie privée en cette fin de XX^e siècle.

⁷. Voir Une question à deux volets : comment améliorer le droit d'accès à l'information tout en renforçant les mesures de protection des renseignements personnels. Rapport du Comité permanent de la Justice et du Solliciteur général (Chambre des communes, Ottawa, 1987) p. 74-77. Voir aussi : L'identité piratée par la Groupe de recherche informatique et droits (Québec, 1986).

⁸. Voir : Data protection act of the State of Hesse of november 11, 86 (Commissaire à la protection des renseignements personnels de Hesse, Wiesbaden, 1987) et le rapport du Comité permanent de la Justice et du Solliciteur général (cf. supra).

⁹. David H. Flaherty : Privacy in colonial New England (Charlottesville, Virginie, 1972).