L'identité piratée

Comment se portent les libertés sur le continent du libéralisme économique ? Comment se passe l'informatisation au pays de la technologie ? Un ouvrage québécois fait le point. Un grand marché de l'information nominative, immergé mais fort bien organisé, géré par des groupes spécialisés au profit des puissances économiques et au détriment d'individus exclus... Là-bas comme ici, l'informatisation doit être maîtrisée.

Il faudra s'y faire : le thème « Informatique et libertés » apparut voilà pourtant une vingtaine d'années, se révèle d'une constante actualité. Pas une année ne se passe sans que ne viennent à l'avant-scène, des violations et des fraudes en tous genres et que l'on ne découvre des dangers encore mal identifiés provenant de la mise en place de nouveaux systèmes. Si le public en général et les fichés en particulier, ne se manifestent guère, ils n'en pensent pas moins si l'on en croit les sondages. Ainsi, une enquête effectuée en 83 montre que la moitié des Américains considèrent que l'ordinateur constitue une menace pour leur vie privée. Les deux tiers estiment que des dossiers sont constitués sur eux dans le plus grand secret. Tout se passe comme si l'on avait sous-estimé l'importance et la difficulté du sujet. L'intervention de lois protectrices et de contre-pouvoirs tels la CNIL en France, s'ils ont apporté une amélioration, ne sont pas à eux seuls capables d'apporter une véritable solution.

Un point central qui aurait mérité une plus grande attention et sur lequel vraisemblablement il faudra revenir, est le droit de propriété de l'individu sur les informations qui le concernent ou en termes plus accommodants, *le droit d'une maîtrise minimale sur les doubles informatiques de sa personnalité stockés dans les fichiers*. Ce droit est certes reconnu au niveau des principes et au plan législatif mais fort timidement, sans que l'on en ait véritablement tiré toutes les conséquences. Aucun effort sérieux n'a été fait pour en informer le public et pour lui donner les moyens de le faire respecter. Cette manière de procéder a l'avantage de ne pas remettre en cause la situation actuelle où ce sont les ficheurs qui se considèrent comme propriétaires des informations qu'ils ont stocké sur les personnes mais présente par contre l'inconvénient, de laisser ces personnes désarmées devant les abus. Ces abus ne peuvent d'ailleurs que se multiplier sous la pression des intérêts administratifs et commerciaux, les grandes organisations ayant trouvé dans l'exclusion de l'individu des procés d'information qui le concerne, une nouvelle forme particulièrement efficace, de gestion et de contrôle social.

Un des intérêts majeurs de l'ouvrage du GRID de Montréal, « l'Identité piratée » est comme son titre l'annonce clairement, de prendre au sérieux cette question de la propriété de l'individu sur ses informations. Réalisée à la demande du Gouvernement du Québec à la suite de la découverte de « listes noires de locataires » mises sur pied par des associations de propriétaires immobiliers, cette étude apporte une triple contribution à l'abondante littérature sur le sujet « informatique et libertés » : elle identifie les grands pirates d'identité actuels et futurs dans un secteur encore insuffisamment exploré, le secteur privé ; elle propose une analyse logique du procès d'information qui permet de prendre toute la mesure de la dépossession actuelle de l'individu ; enfin, après un examen des expériences et réflexions intervenues, elle indique les voies les plus efficaces pour faire face. *

Un marché de l'information nominative

Les pirates ne sont pas ici des individus marginaux mais *de grandes entreprises* qui ont pignon sur rue. Une réglementation existe au Québec pour protéger les renseignements personnels dans le secteur public mais rien ou presque, en ce qui concerne le secteur privé. On trouve aux Etats-Unis une situation comparable avec quelques interventions ponctuelles à l'égard d'entreprises particulièrement menaçantes comme les agences de renseignements. En France et dans d'autres pays européens, la protection concerne aussi bien le secteur public que le secteur privé, ce dernier faisant cependant l'objet d'une moins grande attention. Ainsi par exemple, au moment de la création d'un fichier, une entreprise a simplement l'obligation de le déclarer alors qu'une administration doit y être autorisée. Toujours est-il que les auteurs du GRID montrent qu'un véritable marché de l'information nominative est en voie de constitution où chaque donnée se verra attribuer une valeur marchande. Les institutions financières qui sont les plus actives dans la création de ce marché, sont considérées comme les acteurs les plus menaçants du présent mais surtout, de l'avenir. Plusieurs facteurs concourent à ces phénomènes : tout d'abord, l'accroissement et l'élargissement des actes de consommation ; ensuite, le développement technique avec des outils de plus en plus performants dans l'intégration, le traitement et la diffusion de l'information comme les banques de données relationnelles et les réseaux télématiques.

Ce diagnostic est établi à partir d'une enquête approfondie : entretiens semi-directifs auprès d'une cinquantaine de représentants d'entreprises du secteur financier et de la consommation (banques, compagnies de carte de crédit, agences d'enquête, compagnies d'assurances, maisons de sondage, agences de renseignements sur les consommateurs etc.), sondage sur les fichiers de personnel auprès d'une centaine d'entreprises, réalisation de deux panels avec des associations. Les observations les plus saillantes ont trait d'une part à la découverte d'officines spécialisées dans le recueil et l'intégration de l'information financière et médicale sur les individus et d'autre part, dans le dévoilement des méthodes de gestion et de décision des grands pirates d'identité que sont les banques et les compagnies de cartes de crédit.

** A propos de l'ouvrage du GRID (Groupe de recherche informatique et droit à Montréal), « L'Identité piratée », Ed. Soquij, Montréal.*

Les individus exclus

Le Québec est concerné par deux réseaux principaux d'intégration de l'information sur les personnes. Le premier est le Bureau de crédit qui informe en temps réel les commerces de quelque envergure sur la solvabilité de leurs clients. Plus précisément, cette officine donne pour chaque individu *une cote de crédit qui s'échelonne de 1 à 9*. Elle reçoit en retour pour déterminer ces cotes, des données communiquées par tous les membres du réseau sur les conditions et modalités de paiement de leurs clients. Pratiquement tous les Québecois ont un dossier à ce Bureau de crédit.

Un deuxième réseau est constitué par le Medical information bureau (MIB) qui s'occupe lui, de l'aspect médical de la personnalité. Il intéresse plus particulièrement les compagnies d'assurances sur la vie. Le bureau situé à Boston, informe ces compagnies du degré de santé des assurés potentiels qui frappent à leur porte. En échange, il recevra d'elles, tous les renseignements médicaux qu'elles ont pu obtenir des demandeurs. Ce dernier réseau qui fonctionne au niveau nord-américain, pose clairement le problème de la souveraineté d'un pays sur les informations relatives à ses citoyens et marque d'entrée, les limites d'une réglementation qui n'interviendrait que localement.

La constatation la plus troublante porte sur les méthodes de gestion et de décision des entreprises du secteur financier commes les banques et les compagnies de cartes de crédit. Ces entreprises qui se montrent le plus hostiles à l'intervention d'une réglementation, agissent en dehors de tout contrôle, et constituent selon les auteurs, un véritable Etat dans l'Etat. La masse des données qu'elles traitent est colossale et touchent toute la population. Etant informatiquement les mieux outillées, ce sont elles qui à ce jour, réalisent la plus parfaite exclusion de la personne, des

Les fichiers de « mauvais payeurs »

La situation en France, en ce qui concerne la gestion des crédits ou des prêts consentis à des personnes physiques par des établissements de crédits, peut être résumé de la manière suivante. Une norme simplifiée a été définie par la C.N.I.L. en 1980 ; la C.N.I.L. a procédé à des contrôles qui ont démontré l'existence de débordements, en particulier l'élaboration de manière automatique de scores de l'emprunteur pour décider de l'attribution ou non d'un crédit (le score est le résultat de notes positives ou négatives affectées à chaque élément d'information fournies par le client lors de sa demande de prêt : âge, sexe, vie affective et familliale, emploi, logement, nationalité...). De plus la C.N.I.L. a découvert la pratique nouvelle de l'échange informatisé d'informations entre banques à partir des fichiers des mauvais payeurs. Elle a décidé en 85 de restreindre les possibilités offertes par la norme de 80, en reformulant un certain nombre d'articles *, et en rédigeant une recommandation dans le cas où la banque souhaite aller plus loin que la norme, c'est-à-dire si elle veut intégrer dans son programme un score ou céder des informations. Ces recommandations sont entre autres :

- que toute personne à laquelle un refus de crédit est opposé soit informée, par écrit ou oralement, des raisons de ce refus de façon suffisamment explicite ;
- que les informations nominatives enregistrées dans un fichier des incidents de paiement ne soient pas conservées au-delà d'un délai d'un an à dater de la constatation de l'extinction de la dette ;

Les trois associations bancaires et de crédit françaises ont alors décidé de faire un recours en Conseil d'Etat sur la nouvelle norme et sur la recommandation (ce qui est étonnant car cette dernière n'a pas de caractère obligatoire). Les banques critiquent un excès de pouvoir de la C.N.I.L. sur les restrictions de la nouvelle norme, sur la limitation du temps de conservation des informations à un an (alors que des contrôles ont montré qu'elles gardaient des défauts de paiement, parfois pendant 13 ans !), sur les restrictions d'échange d'informations entre banques et surtout sur le fait que la C.N.I.L. demande à prendre connaissance des informations et de la manière dont sont calculés les scores. Les banques rechignent à fournir à leurs clients qui se voient opposer un refus les raisons de celui-ci ce qui d'une certaine manière est contraire à l'article sur les profils de la loi informatique et libertés et à celui qui permet à toute personne de connaître et de contester les informations et les raisonnements qui lui sont opposés.

La situation en est là, le Conseil d'Etat n'ayant pas encore statué : actuellement les banques ont, semble-t-il, tendance à utiliser la norme, nouvelle mouture, qui permet simplement la gestion et la constitution du dossier de crédit, ou de joindre les éléments du calcul du score lors de leurs déclarations ordinaires faites sans référence à la norme.

Reste que des informations erronées ou trop ancienne, par exemple sur des défauts de paiement, peuvent être utilisées à tort. De plus le demandeur peut se trouver éloigné de ceux qui décident d'attribuer ou non un crédit, comme dans le cas d'une demande formulée depuis un grand magasin, il n'est pas alors en mesure de contester la décision.

Les dispositions légales semblent avoir été prises pour éviter la mise en place de méga-fichiers comme celà existe dans d'autres pays, mais certains seront peut-être tentés de passer outre.

** Voir les textes complets dans le 6e rapport de la C.N.I.L.*

procès d'information qui la concernent. *L'accessibilité* d'une personne à son dossier est ainsi tronquée. Les seules informations communiquées seront celles que le client lui-même a donné à l'exclusion de renseignements provenant d'autres sources comme par exemple, le degré de solvabilité établi par le Bureau de crédit. L'impossibilité pour la personne de valider l'information la concernant augmente les possibilités d'erreurs cumulatives et de dommages clandestins. Or, il est généralement reconnu que les erreurs sont nombreuses dans les grands systèmes. De la même façon, des informations nominatives sont diffusées à l'insu des intéressés et sans leur accord. Ces pratiques qui tendent à exclure toute intervention de la personne, aboutissent à une bureaucratisation du système décisionnel qui présente d'énormes risques : risques psychologiques pour l'individu massifié et spolié de sa véritable identité, risques de dépendance et de fragilisation dus au gigantisme de ce système, risque de débordement des Etats, moins riches en informations que ces entreprises privées. Qui plus est, « au processus de bureaucratisation de la décision s'en ajoute un autre plus grave, qui n'a pas encore pris sa mesure mais qui commence à se mettre en place. De fait la généralisation de guichets automatiques, la généralisation des moyens de paiement électroniques, la mise en place de la carte de paiement qui débitera le compte personnel en temps réel, la généralisation des réseaux bancaires informatiques, vont produire l'automatisation du processus décisionnel. Il ne s'agit même plus de l'exclusion de la personne : « Les agents incarnant le système sont eux-mêmes remplacés par des processus totalement informatisés » (p. 104). Ce type de gestion, si contraire aux droits des personnes, tendra certainement à s'étendre à brefs délais à d'autres secteurs comme les établissements de crédit, les compagnies d'assurance, les fournisseurs de listes d'adresses, les courtiers en valeurs mobilières.

Un procès d'information sous influence

Il est clair que l'innovation technologique n'est pas sans influencer profondément les structures informationnelles. L'approche logique du procès d'information proposée par l'ouvrage présente à cet égard un double avantage : en considérant l'information indépendamment de son support, elle évite de baser l'analyse sur des moyens technologiques par nature transitoires ; elle permet par ailleurs, de bien mettre en lumière à un moment donné, les effets spécifiques d'une technologie particulière. Le recueil, le traitement et la diffusion de l'information sont les grands moments logiques qui conditionnent l'existence même de l'information. « Intervenir de manière permanente signifie nécessairement déterminer les conditions légales du recueil de l'information (c'est la dimension du contenu), du traitement (c'est la dimension des opérations qui produisent l'information en tant que telle), de la diffusion (c'est la dimension où les acteurs sont identifiés) » (p. 35). Cette méthode d'analyse est précieuse pour faire apparaître le vol d'identité dont sont victimes les individus et les effets intégrateurs et normalisateurs de l'informatique.

Le recueil de l'information est fait dans de nombreux cas, à l'insu de la personne. Ainsi opèrent les agences d'enquête et les experts en sinistre qui constituent les dossiers où les données superficielles, partielles voire carrément fausses, sont légion mais ne peuvent à aucun moment être contestées. Les fournisseurs d'adresses recourent également à *une collecte clandestine*. Est-ce normal, s'interrogent les auteurs, qu'une entreprise puisse utiliser dans ces conditions, le nom et l'adresse d'une personne pour en tirer profit ? Le nom et l'adresse sont-ils oui ou non, une propriété individuelle ? Dans le cas de relations contractuelles, les individus connaissent l'existence des dossiers constitués sur eux. Cela n'exclut pourtant pas les abus. En effet, « quelle est la pertinence des informations demandées eu égard au service à donner ? A partir de quand (ou de quelle quantité de renseignements), l'entreprise qui procure le service juge t-elle que l'information recueillie est suffisante ? Avec l'informatisation croissante et la baisse corrélative des coûts de traitement, la limite du recueil ne va-t-elle pas être indéfiniment repoussée ? » (p. 79). On voit ici l'importance de questions généralement ignorées pour le plus grand bien des pirates d'identité. Lorsque la source d'information n'est pas l'individu lui-même, on peut avoir des doutes sur la qualité des renseignements recueillis. D'autant plus que, dans la

généralité des cas, ce sont les renseignements les plus sensibles sur les mœurs, le mode de vie, les opinions qui sont collectés de cette manière indirecte. L'intéressé ne pourra jamais en contester le contenu et en corriger les erreurs dans la mesure où l'accès à son dossier est limité aux informations qu'il a lui-même données. La technique informatique a une influence propre sur cette collecte, dans le sens d'une plus grande normalisation. Elle nécessite en effet la définition de dossiers-type et de descripteurs très précis qui découpent arbitrairement la personnalité et rendent malaisée voire impossible, l'expression des différences.

Une deuxième étape logique a trait *au traitement*. L'informatique a, à ce stade, un impact considérable. En effet, à côté de traitements orientés vers la gestion interne ou vers des organismes officiels extérieurs, l'ordinateur va permettre toutes sortes de croisement, et d'études statistiques. Les fournisseurs de répertoires d'adresses vont parvenir ainsi à une connaissance assez poussée des identités et les grandes entreprises, déterminer différentes *catégories de risques*.

Par exemple, les banques établissent des modèles économétriques prévisionnels et les assurances, des tables de risques. Il est à noter que pour les Québécois, la confection de ce genre de document dans le domaine des assurances-vie, est établi aux Etats-Unis. L'appartenance à un groupe à risque ou l'écart par rapport à une norme statistiquement établie, peuvent motiver une décision défavorable. Le recours à un logiciel d'aide à la décision s'avère quelquefois intéressant dans l'explication des critères et des raisonnements utilisés.

Une dernière étape intéresse la *diffusion et l'échange d'informations* : réseaux internes aux entreprises, réseaux décentralisés d'associés et surtout réseaux externes. Il existe ainsi un réseau international des émetteurs de cartes de crédit qui de même que des officines comme le Medical information bureau, posent très clairement le problème des flux transfrontières.

Des propositions pour faire face

Suite au diagnostic établi, la question se pose de savoir comment rétablir le citoyen dans ses droits et limiter les dangers d'un développement sauvage des banques privées de données sur les personnes. L'étude du GRID ne néglige pas à cet égard les solutions classiques déjà expérimentées ailleurs mais, consciente de leurs limites et sensible à la dimension sociale des enjeux, ne s'en contente pas. A côté de la protection de la vie privée et des renseignements nominatifs, elle préconise des mesures d'une inspiration plus collective afin de contrôler véritablement le phénomène d'informatisation. L'ouvrage se termine par, pas moins de 175 recommandations à l'adresse du Gouvernemnet du Québec.

On sait que de nombreux dispositifs juridiques de protection des renseignements personnels sont intervenus en Europe, en Amérique du Nord et que des organisations internationales comme le Conseil de l'Europe ou l'OCDE, ont fait des recommandations aux Etats membres sur cette question. Une analyse comparative très fouillée dégage l'intérêt et les limites de ces dispositifs et montre le retard du Canada et particulièrement du Québec, dans la réglementation du secteur privé. Comme aux Etats-Unis, une loi de portée générale est intervenue dans le secteur public mais ce dernier pays s'est intéressé aussi au secteur privé en réglementant l'activité des bureaux de crédit et des entreprises du domaine de l'assurance, de la câblodistribution et de l'emploi. En Europe, il existe des lois de protection à portée générale qui concernent aussi bien le secteur privé que le secteur public. Certaines dispositions particulièrement originales sont ici mentionnées : droit des Suédois une fois l'an, à une transcription gratuite de leur dossier, droit de blocage des Allemands leur permettant de contrôler la qualité des renseignements détenus à leur sujet, interdiction française d'utiliser des profils pour fonder une décision judiciaire et dans une moindre mesure, administrative. Il y a urgence pour le Québec à légiférer dans le secteur privé pour protéger la vie privée des individus et leur assurer une maîtrise minimale sur leurs informations. Il suffirait de reprendre les normes préconisées par l'OCDE sur les obligations des gestionnaires de fichiers et sur les droits nouveaux à accorder aux personnes fichées : droit d'information, droit de consentement et droit de contestation. Ce niveau de pro-

tection peut être en effet considéré aujourd'hui comme un « plancher », surtout pour un pays membre de l'OCDE.

Les auteurs recommandent également une politique d'autoréglementation par secteurs et la reconnaissance de droits collectifs permettant au public d'intervenir lors de la conception, de l'utilisation et du développement des systèmes.

Cette dernière proposition ouvre des perspectives nouvelles et apparaît comme seule capable d'améliorer un dispositif conçu jusqu'ici dans une perspective trop individualiste et défensive. L'attribution de droits nouveaux à l'individu ne peut en effet remettre véritablement en cause un fichage déjà effectué mais simplement le moraliser et le rendre moins insupportable. L'évolution technique et l'informatisation croissante de la société appelent aujourd'hui des solutions plus collectives et dynamiques pour ne pas laisser la décision informatique entre les mains des seuls intérêts gestionnaires et économiques. D'autant, que ce n'est pas cette fois la seule vie privée qui est menacée, mais tout un ensemble de prérogatives et de droits. Aussi bien, reconnaissent les auteurs, « les solutions ne peuvent être seulement juridique mais déborder largement sur la mise en place de conditions pour favoriser un débat large et public sur l'informatique en tant que phénomène de société, et sur les mesures susceptibles d'en assurer la maîtrise et le contrôle social, telles la recherche, l'éducation ainsi que l'accès à l'expertise, la participation et l'implication des associations et des groupes représentant les intérêts des citoyens ».

Sur ce terrain-là tout reste à faire au Québec et ailleurs, mais la voie est clairement indiquée et la lecture de « L'identité piratée » nous convainc qu'il y a urgence et nécessité.

ANDRE VITALIS

Carte d'identité informatisée : où en est-on ?

Le 1er juillet 1986 la C.N.I.L. avait rendu un avis sur le projet de décret du Ministère de l'Intérieur visant à créer une carte d'identité informatisée (voir Terminal n° 30). En ce qui concerne le relevé d'une empreinte digitale lors de la demande de carte (empreinte qui serait « conservée au dossier par le service gestionnaire de la carte ») la C.N.I.L. avait décidé de « surseoir à statuer » ; dans son rapport, M. Jacques Thyraud, sénateur (R.I.) du Loir-et-Cher, après un exposé des différents motifs (techniques et juridiques) en arrivait à la conclusion : *« Toutes ces raisons font que la constitution d'un fichier national d'empreintes digitales monodactylaires n'est pas possible aux yeux de votre rapporteur ».*

Saisie à nouveau par le Ministère de l'Intérieur, la C.N.I.L. va rendre le 21 octobre 1986, un deuxième avis qui, malgré la position dévavorable du rapporteur, autorise la prise d'une empreinte digitale. Cette autorisation est assortie de deux conditions : i ne peut être constitué un fichier des empreintes digitales, manuel, mécanographique ou automatisé, centralisé au niveau national et il ne sera pas procédé à la numérisation des empreintes digitales enregistrées dans les fichiers départementaux.

Dans cet avis, la C.N.I.L. demande en outre que « les actes de naissance, nécessaires à la délivrance de la carte national d'identité, soient demandés directement par les préfectures aux mairies ». Ce point est important. En effet, dans son rapport du 1er juillet, M. Thyraud justifiait la mise en place d'un fichier national informatisé pour deux raisons : *«l'attribution à chaque carte d'un numéro informatisé par rapport à la personne » et pour lutter « contre une fraude par usurpation d'état-civil ».* la proposition de la C.N.I.L. (demande des actes de naissance par la préfecture aux mairies) permet de mieux combattre l'usurpation d'état-civil que le fichier informatisé. Reste l'attribution du numéro de la carte. Notons à ce propos que les cartes d'identités actuelles ont un numéro dont l'attribution se fait manuellement.

Par conséquent, après les deux avis de la C.N.I.L., et si l'on prend en compte ses recommandations, il n'existe plus aucune raison sérieuse qui puisse justifier la création au Ministère de l'Intérieur d'un fichier national informatisé, véritable état-civil parrallèle. Si ce fichier était maintenu, on pourrait alors se poser la question : quelle sera réellement son utilisation ? Un tel fichier centralisé n'a d'ailleurs pas été retenu pour la carte d'identité infalsifiable en Allemagne, pays pourtant « expert » dans le développement des systèmes informatiques sécuritaires.

Le 19 mars 1987 le gouvernement a pris deux décrets ; l'un portant *« création d'un système de fabrication et de gestion informatisée des cartes nationales d'identité »*, l'autre relatif au *« relevé d'une empreinte digitale lors d'une demande de carte nationale d'identité ».* Bien que ces décrets respectent les avis de la C.N.I.L., il n'en subsiste pas moins trois problèmes :

- La création d'un fichier national informatisé, concernant à terme toute la population française qui, comme nous l'avons vu plus haut, ne présente plus aucune utilité dans la lutte contre la falsification des cartes d'identité.

On comprend mal dans ces conditions pourquoi la C.N.I.L.' a émis un avis favorable à la création d'un tel système informatisé dont le coût, par ailleurs, n'est pas négligeable.

- La prise d'une empreinte digitale à propos de laquelle le rapporteur de la C.N.I.L. affirmait : *« la France ne doit pas se doter d'un fichier de masse, même éclaté d'empreintes digitales monodactylaires ».*
- La police et la gendarmerie pourront accéder, à l'aide de la carte d'identité, au Fichier des Personnes Recherchées pour lequel la C.N.I.L. n'a pas encore rendu d'avis.

La carte d'identité a ainsi plusieurs finalités, ce que la C.N.I.L. avait refusé en 1980. Pour autant, selon Charles Pasqua, les premières cartes d'identité informatisées seront mises en circulation avant la fin de l'année.

JEAN-PIERRE DEMO