

Informatique et liberté

Autor(en): **Maisonrouge, J.-G.**

Objektyp: **Article**

Zeitschrift: **Revue économique et sociale : bulletin de la Société d'Etudes Economiques et Sociales**

Band (Jahr): **39 (1981)**

Heft 4

PDF erstellt am: **09.08.2024**

Persistenter Link: <https://doi.org/10.5169/seals-138694>

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Informatique et liberté

J.-G. Maisonrouge,
président directeur général,
IBM-Europe, Paris

Le commencement de la réflexion politico-philosophique sur le sujet de la liberté se perd dans la nuit des temps. Et aucun d'entre nous n'en verra la fin. Chaque événement susceptible d'exercer une influence sur cette sphère d'autonomie propre à l'homme, vient donner au débat une direction nouvelle. C'est le cas de l'informatique.

I. PROBLÉMATIQUE

L'informatique est devenue un fait de société, nul ne peut le nier. Les nombreux débats d'idées, nationaux et internationaux, qu'elle suscite en témoignent largement. Ils cherchent tous des réponses à la même question: quel avenir le développement de l'informatique prépare-t-il?

Notre siècle vit actuellement la rencontre de trois évolutions:

- D'une part, les technologies informatiques, apparues il y a plus de trente ans, n'ont cessé de se transformer pour s'introduire aujourd'hui dans presque tous les domaines de la vie quotidienne. Il y a aujourd'hui plus de 500 000 ordinateurs personnels installés aux USA.
- D'autre part, la critique du modèle de croissance industrielle, critique qui a bien diminué lorsque les taux de croissance ont baissé, laisse apparaître une aspiration très forte à de nouveaux rapports entre l'individu et la société.
- Enfin, les répercussions de plusieurs années de difficultés économiques accélèrent la modification des valeurs culturelles. La recherche d'une meilleure qualité de la vie prend le pas sur la quête effrénée de satisfactions essentiellement matérielles, surtout pour les citoyens des pays développés qui ont atteint déjà un standard de vie élevé.

L'heure des choix est arrivée pour les sociétés occidentales. Nous devons dès à présent construire le Futur.

De tous temps, les hommes ont utilisé les techniques qu'ils inventaient pour atteindre leurs objectifs économiques, sociaux et culturels. L'informatique est désormais une nouvelle technologie entre leurs mains. A ce titre et en raison de sa diffusion rapide, elle s'impose comme facteur de changement.

L'ordinateur crée une situation nouvelle dans la mesure où il permet le rassemblement, l'analyse et la communication d'informations, très nombreuses et complexes. Il permet donc de savoir plus, mieux et plus vite. Et *savoir*, écrivait Teilhard de Chardin, permet de *pouvoir*.

Mais si le rôle croissant de l'information renforce l'acuité de ce sujet, celui de la relation entre le savoir et le pouvoir, il ne faut pas voir dans l'ordinateur autre chose qu'un support de la connaissance. Car, ne nous laissons pas entraîner par la puissance des mots, ni par l'émotion que suscitent les titres spectaculaires des journaux, les produits de l'industrie informatique ne sont que des outils. Pour que l'information soit transformée en pouvoir, il faut un acte politique. Cet acte, cette décision, appartiennent à l'homme seul. Raisonner autrement serait confondre l'outil et son utilisation.

C'est l'utilisation de l'ordinateur qui pourrait effectivement conduire à des abus. Le risque existe. L'atteinte aux libertés individuelles en est un. Le risque sera conjuré si la volonté de contrôle existe. Et elle existe. Les réglementations nationales et internationales le prouvent.

II. LIBERTÉ ET VIE PRIVÉE

L'histoire de l'homme est en grande partie celle de sa lutte pour la liberté. Du suicide de Socrate à la Grande Charte, de la Révolution française à la Déclaration des droits de l'homme, le grand héritage du monde occidental est la croyance en la liberté individuelle. Mais chacun sait que la liberté est fragile. Il faut mener un combat quotidien pour la protéger, même dans les démocraties les plus évoluées.

La liberté est vue comme un ensemble de droits: droit d'accession à la propriété, droit d'expression, droit à la sécurité. C'est encore le droit de faire ce que l'on veut sans mettre en cause les droits des autres, selon l'adage qui veut que «sa propre liberté s'arrête où commence celle des autres».

Et, il y a aussi le droit à la protection de la vie privée. Notion d'ailleurs difficile à définir. Les juristes semblent faire leur, sans le savoir peut-être, cette maxime de l'empereur Justinien concernant le droit ancien: «Dans le droit civil, toute définition est périlleuse». Pourtant, beaucoup ont essayé de proposer une telle définition.

Le professeur Alan Westin tente une approche anthropologique en définissant la vie privée comme «un besoin de solitude, d'intimité, d'anonymat, de distance». On peut encore dire, comme un ancien ministre de la Justice français, que c'est «l'aspect de l'existence d'une personne que celle-ci ne veut pas rendre public».

Il est vrai que la notion de vie privée se prête mal au cadre formel de la définition, tant elle recouvre d'aspects multiples et relatifs. Chacun de nous en a l'intuition. Chacun de nous a des idées personnelles sur ce qu'est sa vie privée. C'est tout.

D'ailleurs, l'intérêt pour la notion de vie privée est très récent. Ignorée de l'Antiquité, elle n'apparaît qu'avec la fin de la féodalité. Elle ne commence à devenir un sujet de préoccupation qu'à partir de la fin du XIX^e siècle, pour prendre une importance réelle, dans les pays occidentaux, après la Seconde Guerre mondiale. Nous sommes donc en face d'une absence de définition légale. Mais, et c'est là l'important, le droit de chaque individu au respect de sa vie privée est formellement reconnu.

Par l'Assemblée générale des Nations Unies d'abord, qui adopte, en 1948, la Déclaration universelle des droits de l'homme. Puis par le Conseil de l'Europe en 1950, qui signe la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. Les deux textes affirment, «le droit de toute personne au respect de sa vie privée». Faisant suite aux travaux de la communauté internationale, différents pays ont élaboré des textes consacrant ce même droit. C'est le cas de l'Allemagne, et celui de la France, qui, en 1970, a introduit dans son code civil l'article 9 stipulant que «chacun a droit au respect de sa vie privée».

Ce droit est également reconnu aux Etats-Unis, même si sa définition varie d'un Etat à l'autre. Par contre, les auteurs du rapport canadien «L'ordinateur et la vie privée» voient là un problème politique et non juridique. Et, en Angleterre, le rapport Younger constate que la «Common Law» n'apporte pas de solution satisfaisante.

La jurisprudence vient donc parfois combler les carences du droit positif. Je donnerais comme exemples les sanctions prononcées en cas d'atteintes portées au secret de la vie privée par la publication non autorisée de photographies, consacrant ainsi le droit de l'individu à son image. La jurisprudence américaine a été la première à œuvrer dans ce sens. Elle fut imitée ensuite par tous les pays occidentaux.

Mais je dirais qu'en réalité la protection de la vie privée est plus qu'un droit. C'est une nécessité psychologique. C'est aussi une sauvegarde de la démocratie. Car la grande crainte est celle de la surveillance de nos activités que le non-respect de ce droit peut entraîner. Surveillance exercée par la puissance publique au nom de l'efficacité administrative ou de la sécurité. Ou encore par des individus ou des groupes sans scrupules.

III. L'ORDINATEUR CONSTITUE-T-IL UNE MENACE ?

La création de fichiers réunissant des informations personnelles sur les individus n'est pas récente. En fait, depuis l'invention de l'écriture, il existe des fichiers, essentiellement tenus par les pouvoirs publics. Parce que les hommes oublient. La seule mémoire réputée infaillible est le fichier.

Sur quoi les tribunaux ou les administrations appuient-ils généralement leurs décisions ? Sur l'observation des faits, mais aussi sur la connaissance et l'extrapolation du passé. Le fichier s'impose donc comme le recours indispensable face aux défaillances de la mémoire humaine. Il s'impose d'autant plus aujourd'hui que l'information est nécessaire au gouvernement des sociétés.

Manuels pendant longtemps, les fichiers présentaient déjà des risques potentiels auxquels l'individu se trouvait nécessairement exposé. Traditionnellement, les divers fichiers que les lois ont rendus obligatoires — je veux parler des fichiers de recensement, des impôts, de la sécurité sociale, de la police — ou encore les fichiers médicaux ou bancaires étaient décentralisés. Notre protection était en partie due à l'inefficacité et aux difficultés de communication entre les différentes parties prenantes.

Aujourd'hui, ces fichiers sont largement automatisés. Les progrès très rapides de la technologie informatique permettent la création de grandes banques de données centralisées et l'accès direct à un nombre considérable d'informations à partir des terminaux. Ces mêmes

progrès sont à l'origine du développement des réseaux, circonscrits aux frontières d'un pays ou étendus sur plusieurs Etats.

La télématique, en favorisant la circulation des informations au-delà des frontières nationales, crée une situation nouvelle en termes de volume de données transportées. Prenons divers exemples pour évaluer l'importance de ces banques de données.

Aux Etats-Unis, où le parc d'ordinateurs est le plus important :

- La Direction des impôts conserve toutes les données fiscales de 80 millions d'Américains.
- La Sécurité sociale a des renseignements détaillés sur les salaires de 95 millions de personnes.
- Le FBI dispose des empreintes digitales de 86 millions de personnes.
- Les Services secrets ont des informations précises sur 50 000 personnes susceptibles de mettre en danger la vie de certaines personnalités. Et ainsi de suite...

En France, on dit qu'il existe environ 100 000 fichiers automatisés de personnes. Chaque Français est connu par au moins dix organismes de taille nationale, sans compter divers fournisseurs dont l'activité peut s'exercer sur tout le territoire. Cela va de l'école à la compagnie d'assurance, des impôts à l'armée, de la banque au téléphone, etc. C'est donc la multiplication et l'éventuelle interconnexion de ces fichiers, rendues possibles par l'informatique, qui émeuvent l'opinion publique.

Le danger, pour certains, vient de ce que la constitution et la consultation de fichiers tend à se banaliser. On a peur que le recours à un identifiant unique puisse faciliter le croisement entre les fichiers et modifier la valeur des informations a priori les plus anodines. Mais l'identifiant ne change rien au problème, car dans l'informatique moderne il est aussi facile d'utiliser un nom qu'un numéro de code. Ce qui revient à poser la question suivante : le seul fait de l'intervention de l'ordinateur donnerait-il aux renseignements qu'il stocke et qu'il fournit une autorité supérieure ?

Une autre inquiétude vient de la méconnaissance des fichiers existants et de la fiabilité des informations qu'ils renferment. Certains pensent, en effet, qu'il est plus facile de contrôler les modifications faites sur un dossier classique, tandis qu'on ne peut pas détecter les altérations apportées à des informations enregistrées électroniquement.

En d'autres termes, on craint :

- Que des informations erronées soient enregistrées sans possibilité d'en demander la rectification.
- Qu'une personne non autorisée ait accès à des renseignements confidentiels.
- On craint surtout qu'il soit trop facile de tout savoir.

Nous, constructeurs, sommes très conscients de ces problèmes. Non seulement parce qu'ils sont au cœur des débats sur notre industrie, mais aussi parce que, nous sommes des citoyens responsables, très attachés au concept de liberté individuelle. Nous savons que tous les grands progrès technologiques portent en eux un danger potentiel. Nous savons aussi qu'il faut apprendre à les maîtriser. Mais si l'utilisation de fichiers ou de banques de données comporte des risques réels, elle présente également de grands avantages.

Certains fichiers électroniques rendent des services considérables :

- Au Centre médical de l'Université de Californie, une banque de données est utilisée pour l'inventaire des reins qui peuvent être greffés. L'ordinateur permet à tous les centres de transplantation des Etats-Unis de trouver les organes compatibles.
- En France, un Centre de recherche contre le cancer possède d'importantes bases de données utiles au dépistage et au diagnostic de cette maladie.
- Les fichiers de malades créés par de nombreux hôpitaux font gagner un temps considérable lorsqu'un ancien patient se présente et évitent bien des erreurs.
- En matière criminelle, les ordinateurs apportent aussi une aide non négligeable.

Je tiens à répéter que l'ordinateur n'est qu'une machine, non créative, fonctionnant à l'aide de programmes élaborés par l'homme. Il recueille, enregistre, classe des données, et les restitue sous la forme demandée. Qui songe à condamner l'appareil photographique parce que des photographies indiscretes paraissent ici et là dans les journaux ? Rend-on l'automobile elle-même responsable des accidents qui causent chaque année des milliers de morts ? Seulement, les règles d'utilisation ont été édictées, dans l'intérêt de la société, comme le code de la route et les limitations de vitesse. Cette approche est également valable pour l'informatique.

Nous savons que l'ordinateur peut renforcer les moyens du pouvoir. Alors, puisque ce sont les hommes qui décident de ce que l'ordinateur fera, il appartient aux hommes d'établir les sauvegardes qui les protégeront des abus possibles de l'utilisation de cet outil.

IV. DES LOIS ET DES CODES

Je voudrais souligner un fait rarement énoncé. Je ne crois pas qu'il existe à ce jour aucune référence possible à une nouvelle forme d'abus portant atteinte aux libertés individuelles, due à l'utilisation de fichiers automatisés. Toute réglementation en la matière a donc un rôle essentiellement préventif.

Depuis dix ans, nombre de pays votent des lois réglementant l'utilisation de fichiers automatisés. Dans plusieurs cas, ce fut sous la pression de l'opinion publique et des mass media. La presse a notamment joué un rôle de détonateur en République fédérale d'Allemagne avec la publication par «Der Spiegel» d'un article intitulé «Un monde à la King Kong» donnant une vision apocalyptique du développement de l'informatique dans les administrations.

Les premières législations nationales dites «Informatique et Libertés» datent du début des années 1970 :

- Le précurseur fut le Land de Hesse, en Allemagne fédérale, qui édicta une loi sur la protection des données en 1970.
- La Suède le suivit en 1973.
- Le «Privacy Act» américain fut adopté en 1974.
- La République fédérale d'Allemagne promulgua, en 1977, une loi protégeant l'individu contre l'usage abusif des données nominatives dans les traitements informatiques.

- Le Canada adopta, également en 1977, le «Canadian Human Rights Act».
- En 1978, c'est le vote par la France de la «Loi relative à l'informatique, aux fichiers et aux libertés».
- Toujours en 1978, le Danemark, la Norvège et l'Autriche se dotent de lois similaires.
- L'année suivante, c'est au tour du Luxembourg.
- Le dernier en date est Israël, ce qui porte à neuf le nombre de pays ayant légiféré sur cette question.

D'autres pays, l'Espagne, le Portugal, l'Autriche ont introduit des dispositions constitutionnelles. Des dispositions identiques sont à l'étude aux Pays-Bas. En Suisse, divers cantons (Genève, Bâle, Vaud, Zurich entre autres) disposent actuellement d'un statut protecteur dans ce domaine mais la loi fédérale est toujours en discussion. Dans l'optique de cette loi, la Confédération helvétique a édicté en mars dernier des directives applicables au traitement des données personnelles dans l'administration fédérale. Elles prendront effet le 1^{er} juillet 1981. Il faut également citer quelques pays comme les Pays-Bas, le Royaume-Uni, le Japon, la Finlande ou l'Australie, qui ont élaboré des avant-projets de lois ou bien des rapports de commission.

Enfin, en septembre dernier, les pays de l'OCDE et le Conseil de l'Europe ont adopté des conventions allant dans le même sens que les législations nationales. Elles couvrent, en outre, la question des flux de données transfrontières.

L'analyse des principales lois existantes fait apparaître un certain nombre de principes communs :

- Elles s'appliquent à la fois au secteur public et au secteur privé, avec des modalités différentes.
- Elles supposent la connaissance des fichiers existants et futurs, et instituent l'obligation de déclaration ou d'autorisation selon les cas.
- Elles définissent la nature des informations dont l'enregistrement est autorisé ainsi que la finalité de leur utilisation.
- Elles établissent des sanctions pénales en cas de violation de la loi.
- Toutes ces lois prévoient la constitution d'une autorité de surveillance disposant d'un pouvoir réglementaire. C'est la Commission d'inspection des données en Suède ou la Commission nationale de l'informatique et des libertés en France.
- Enfin, elles donnent à tout citoyen le droit de contrôler les informations le concernant, et d'en demander, si besoin est, la modification ou l'effacement.

Je vois dans ce dernier aspect un progrès important de la démocratie, à mettre au compte de l'informatique. En légitimant le droit à l'information, on met en cause le principe du secret, caractéristique de bien des systèmes législatifs et administratifs.

«La liberté est le droit de faire tout ce que les lois permettent», dit Montesquieu. A présent, nous avons des lois. Elles doivent être respectées par tous et notamment par les professionnels de l'informatique. Ils ont un rôle important à jouer car la protection des données dépend pour une grande part de leur intégrité.

Certains gouvernements pensent d'ailleurs que l'efficacité de cette protection dépend avant tout du bon comportement de ces techniciens. La Grande-Bretagne semble s'orienter dans cette voie, sous l'impulsion d'une association professionnelle, la «British Computer Society», qui souhaite la création d'un ordre des informaticiens. Ceux-ci se verraient contraints de s'y inscrire pour exercer leur profession et une juridiction interne sanctionnerait les fautes.

Il est souhaitable que l'approche autorégulatrice s'étende, à condition toutefois qu'elle écarte les risques de corporatisme. Les codes de déontologie constitueront alors un complément indispensable de l'approche institutionnelle.

V. LA SÉCURITÉ DES DONNÉES

La question de l'atteinte éventuelle à la vie privée ne peut être dissociée de la sécurité des données, qui relève de la qualité des systèmes physiques de protection et de celle des procédures. La responsabilité en incombe aux utilisateurs et aux constructeurs.

1. Les utilisateurs

Les industriels s'efforcent depuis longtemps de protéger la confidentialité de leurs méthodes de fabrication ou des résultats de leur recherche. La protection physique de leurs systèmes informatiques, donc de leurs informations, n'est pas un problème nouveau. C'est une préoccupation supplémentaire. Seul l'utilisateur est en mesure d'évaluer le risque, en sachant qu'une source éventuelle d'erreur, de fraude ou de perte d'information a plus de chance de se produire en amont ou en aval de son ordinateur, qu'au niveau de celui-ci.

IBM a procédé en 1975 à une importante étude sur ce sujet en collaboration avec le Gouvernement suédois. Les conclusions restent valables six ans après. La méthodologie adoptée a permis de classer les situations susceptibles de présenter des risques pour la sécurité des données, en trois catégories :

- La manipulation des équipements informatiques,
- l'exploitation du système,
- l'environnement.

A chacune de ces situations correspondent des protections possibles.

Si le problème se complique avec le développement de la télématique, en raison de la circulation des données sur les lignes téléphoniques, il n'en existe pas moins des méthodes de protection appropriées. Essayez de demander, au guichet d'une compagnie aérienne équipé de terminaux, la liste des passagers d'un vol donné ! Vous ne l'obtiendrez pas. Soit parce que le règlement de la compagnie aérienne l'interdit, soit parce que l'opérateur n'aura pas, techniquement, les moyens de vous répondre. Dans ce cas, le constructeur aura fourni, avec la machine, des dispositifs de protection de nature technologique.

2. Les constructeurs

Les progrès de la technique permettent aux utilisateurs de disposer de tous les niveaux de protection souhaités. Conscients de l'importance du problème, nous avons beaucoup investi dans cette recherche.

De très nombreuses méthodes existent déjà, qu'il s'agisse de clés d'accès, de procédés d'identification de l'opérateur, d'accès sélectif. Certains systèmes permettent aussi la détection de tentatives d'accès non autorisées, grâce à un contrôle systématique des transactions. La liste serait longue des méthodes de protection disponibles.

Il en est une que je voudrais citer, car sa mise au point par IBM fut la conséquence directe de l'accroissement considérable du télétraitement. Il s'agit d'un dispositif de cryptage appelé «Data Encryption Standard». Il rend inintelligible et indécodable tout message circulant entre une station émettrice et une station réceptrice. Il a été homologué aux Etats-Unis par le National Bureau of Standards. Dois-je souligner que ces méthodes de contrôle sont incomparablement plus efficaces que celles utilisées pour les fichiers manuels... Quand elles existent.

Nos investissements dans ce domaine sont nés de la conviction que la responsabilité du législateur est de décider qui a accès à quoi, et celle du constructeur de mettre au point les techniques de préservation des bases de données, afin de pouvoir en réserver l'accès à ceux-là seuls qui y ont droit. Dès lors, puisque l'utilisation de l'ordinateur a donné lieu à des lois et puisque des sauvegardes technologiques ont été incorporées, l'ordinateur peut être considéré comme le garant de la protection des fichiers. Au lieu de représenter une menace pour la vie privée, n'est-il pas plutôt à mettre au rang des moyens capables de la protéger?

VI. CONCLUSION

L'Europe va être, dans les années qui viennent, le champ d'une véritable explosion informatique.

Les résultats d'une étude européenne réalisée pour le compte des Postes et Télécommunications indiquent que le volume des données traitées par des moyens informatiques va être multiplié au moins par dix d'ici 1985 et qu'à la même époque il y aura 173 millions de terminaux installés. Cette même étude prévoit que 13 000 entreprises et administrations disposeront de réseaux internationaux permettant la transmission de soixante-dix millions de mots par jour. Ces chiffres sont impressionnants. Ils prouvent que nous sommes à l'aube d'un changement de dimensions en terme de besoin d'information.

Il faut conclure, non à une augmentation des abus possibles au regard des libertés, mais à un renforcement du rôle de l'information dans nos sociétés modernes. En tant que fournisseurs et utilisateurs de matériel informatique, parce que nous estimons que c'est notre devoir, nous coopérons avec toutes les instances nationales et internationales. Mais il serait regrettable que, faisant le procès de l'informatique, des règlements mal adaptés compromettent les besoins légitimes des sociétés en cours d'informatisation.

Il n'est pas dans l'intérêt du développement de l'informatique que celle-ci soit présentée comme un instrument d'atteinte aux libertés individuelles. Ce n'est pas le scalpel qui est responsable d'une mauvaise opération, c'est le chirurgien. Ce n'est pas la machine à écrire qui est responsable d'un article diffamatoire, c'est son auteur. Ce n'est pas l'ordinateur qui menace notre liberté individuelle, c'est l'homme.

Pourquoi entend-on encore dire ici et là : «C'est la faute de l'ordinateur»? On oublie trop souvent que les lois s'appliquent au comportement des hommes, non aux machines. Une machine ne peut décider d'elle-même de nuire à autrui. L'homme le peut. Georges Duhamel l'avait très bien compris : «Je ne me défie pas de la machine que je regarde avec curiosité sur son socle ou sous sa verrière. Je me défie de la machine qui est en moi. Je me défie de ma façon d'employer la machine.»

Mais n'accusons pas l'homme de tous les maux. Lorsque Columbia a raté son premier départ, la plupart des articles étaient intitulés «Les ordinateurs ont failli à leur mission». Après l'exploit extraordinaire que l'on sait, on a rendu hommage aux hommes. C'est mieux ainsi puisque l'opinion a reconnu que c'était l'intelligence humaine qui avait, une fois de plus, triomphé de la machine.