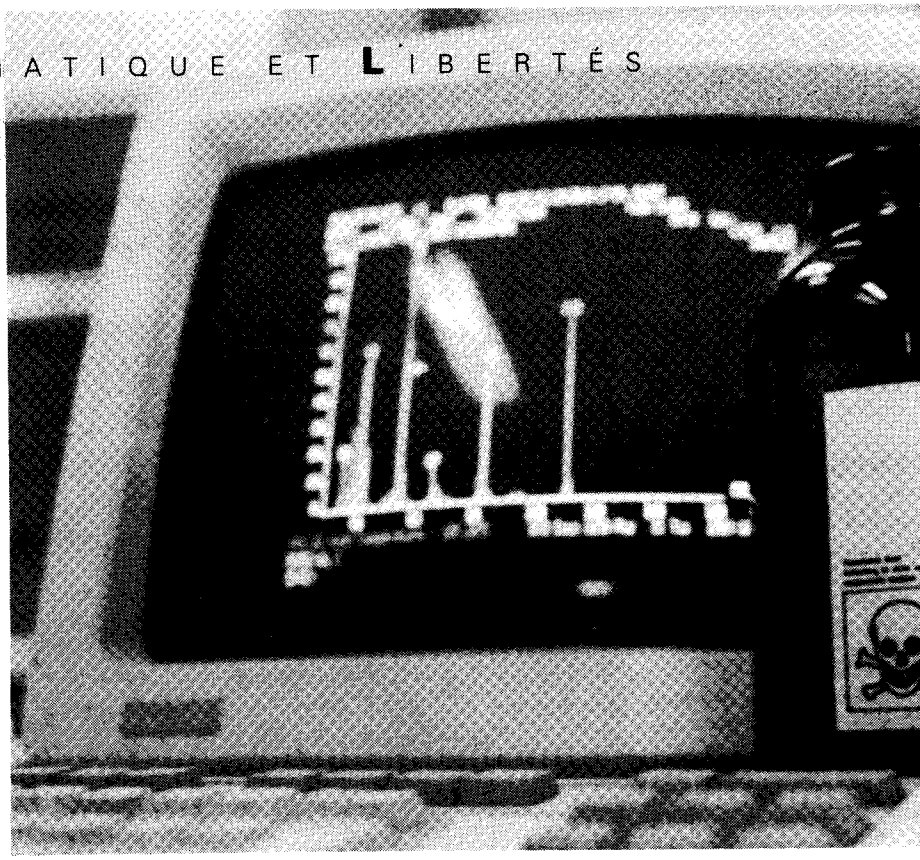
La protection des données hospitalières



PAR DANIEL ROULET ET CONSTANTIN JORNOT *

Le problème de la protection des données ne se pose pas tout à fait de la même manière dans un environnement hospitalier et dans une entreprise bancaire. D'une part, parce que les données qui sont collectées (de manière informatique ou pas) sont considérées comme particulièrement sensibles dans un hôpital. Elles touchent à la sphère la plus intime de la personne. D'autre part, parce que les gens qui collectent ou organisent la collecte de ce genre de données bénéficient en général d'un prestige social plus important que d'autres.

Ces deux raisons font que la législation sur la protection des données en milieu hospitalier est spécifique et l'accès beaucoup plus restrictif que pour les autres données (1) (à part les données de police, ce qui est une autre question). Pour le moment, en milieu hospitalier, on peut dire que les cas d'accès inautorisés et de destruction volontaire de données sont rares. C'est pour que cette situation se perpétue que les quelques considérations qui vont suivre sont nécessaires.

Qu'est-ce qu'un SIH ?

Depuis la fin des années 70, plusieurs grands hôpitaux universitaires dans le monde ont développé un SIH (Système d'information hospitalier), c'est-à-dire un système qui permette non seulement de résoudre les problèmes de gestion quotidienne d'une grande entreprise mais aussi d'offrir aux soignants une aide à leur travail en rapport avec la complexité des sous-systèmes dans lesquels ils sont englobés.

Les SIH les plus élaborés sont aujourd'hui tous centrés sur une banque de données de patients et travaillent en temps réel. Ils permettent d'avoir à tout moment une vue d'ensemble sur la situation des patients (leur mouvement d'une unité dans une autre), des prestations qui leur sont dues ou qui ont été fournies (laboratoires, x-ray). Il s'agit donc de beaucoup plus que d'un système d'administration des patients comme on le trouve dans un cabinet médical ou dans une clinique.

Parmi les nouvelles fonctions que le SIH des années 90 veut englober, on en trouvera deux principales: l'imagerie numérique (PACS) et le traitement automatique du dossier médical (2).

Pour le moment, les données stockées dans un SIH concernent : l'identité détaillée du patient ; l'historique de sa localisation dans l'institution ; ses pathologies ; le résultat de ses examens de labos et autres.

Les avantages du SIH

Il est très difficile de faire l'analyse du SIH en termes de coût-bénéfice même si cela a été tenté. Ainsi on a pu dire que le SIH diminuait la durée de séjour du patient donc son coût ce qui n'est probablement pas une mesure intéressante. On a pu dire aussi que le SIH réduisait le travail administratif des soignants ce qui leur permettait de consacrer plus de temps aux malades. On a dit aussi que le SIH permet de diminuer le gigantisme d'une institution en accroissant la communication entre les membres de la communauté hospitalière, de diminuer les effectifs du personnel administratif, de calculer le coût des soins, etc, ...

* *Centre d'informatique hospitalière, Hôpital universitaire de Genève, CH-1211 Genève 4 - Suisse*

Tous ces avantages sont en partie exacts mais ils sont aussi des justifications *a posteriori* et ils varient sensiblement suivant l'auditoire auquel ils sont adressés. D'autres avantages qui furent présentés au début de la mise en place des SIH, comme la diminution du papier ou l'exactitude des données, ont dû être abandonnés au cours de l'histoire des SIH. Finalement, la seule bonne raison qui reste, c'est que le SIH gère la complexité d'une institution au profit d'une seule figure qui doit rester centrale: le patient. Ce point est très important et il justifie à lui seul que le cas du SIH ne soit pas traité de la même manière que n'importe quel système d'information.

Les menaces contre les données du SIH

Les quelques SIH véritablement intégrés qui existent de par le monde ont su se rendre tellement indispensables qu'on doit garantir leur fonctionnement 24 heures sur 24 et 7 jours par semaine. On admet actuellement que le non-fonctionnement d'un tel système pendant une période qui dépasserait la semaine mettrait définitivement en jeu son existence, sans parler de l'existence de l'institution et de celle des patients, ce qui est bien sûr le plus grave.

Pour analyser les interventions volontaires contre un SIH, il faut partir d'une analyse de ceux qui en veulent au cœur du système, c'est-à-dire au patient. L'énumération des acteurs dangereux potentiels est faite ci-dessous sans *a priori* moral. Les voici donc:

- **Les assurances ou plus généralement ceux qui paient les coûts d'hospitalisation du patient** : Les assurances recherchent particulièrement des listes de patients dont la pathologie peut devenir trop coûteuse (pour s'en débarasser) ou au contraire des listes de patients qui représentent une source de profits potentiels. Elles sont intéressées à reproduire chez elles un sous-ensemble du SIH qui leur permette de calculer plus précisément les coûts futurs et les profits immédiats.

- **Les mass média.** Leur curiosité toujours à la recherche d'un scoop se nourrirait volontiers du nom de quelque patient célèbre pour augmenter leur taux d'écoute ou leur tirage.

- **Les employeurs.** La force de travail doit être en bonne santé quand elle est échangée contre un salaire, mais elle doit aussi être exempte de toute menace à long terme comme les maladies dégénératives ou le HIV positif.

- **Les patients eux-mêmes.** Même si des données ont été collectées avec le plus de soin possible, il peut apparaître au patient qu'une donnée qui le concerne est inexacte ou périmée. Il craint donc qu'elle ne tombe dans le domaine public, veut s'assurer de sa qualité ou mettre en cause son existence.

- **Les auteurs du système** (informaticiens) ou les utilisateurs fréquents de celui-ci. Dans ce cas, c'est la facilité relative d'accès qui crée la possibilité de la fraude. A l'occasion de l'hospitalisation d'un proche, il peut arriver que cette catégorie de personnel abuse de son droit d'accès.

- **Les personnes malveillantes,** c'est-à-dire toutes celles qui s'attaquent à l'informatique en général et non pas au SIH en particulier, ni au patient lui-même.

Bien sûr toutes ces catégories qui peuvent intervenir contre les données du SIH, n'ont pas les mêmes chances de succès. Les plus privilégiées, et le recensement des cas le montre, sont les informaticiens eux-mêmes. Contre eux, la force brute ne sert à rien.

Les stratégies de protection

Face à ces différentes menaces, les responsables de SIH ont élaboré suivant leur perception, trois types de stratégie.

La première approche, historiquement, mais aussi la plus répandue est l'approche sécuritaire qu'on peut caricaturer en l'appelant "parano sécuritaire". Il s'agit en général d'une panoplie de mesures appuyée surtout sur la protection physique du site central, sur les gadgets de hardware variés et sur tout une gestion de type "check-list" de l'exploitation du système.

Cette stratégie a déjà été critiquée (3) non pas parce qu'elle est inefficace par son aspect dissuasif, mais parce qu'elle ne tient pas compte de la spécificité du SIH. On ne protège pas un SIH avec les mêmes motivations qu'on protège la banque du Vatican. En outre, deux facteurs de l'évolution technologique, la miniaturisation et l'architecture des réseaux, font que cette stratégie se révèle comme une perpétuelle course aux nouvelles dépenses d'équipements de protection. D'autre part, l'utilisation des techniques de l'intelligence artificielle dans la pose de virus (4) fait encore perdre de son importance à cette approche.

La deuxième approche est celle du risk management. Elle est de plus en plus répandue et propagée, notamment au niveau européen par les compagnies d'assurances qui proposent leurs services aussi aux hôpitaux. Il s'agit en gros de calculer les risques en définissant ce qui est acceptable et ce qui doit être assuré. Grâce à une série de techniques elles-mêmes informatisées, on procède ensuite à des investissements de sécurité aussi bien hard que soft par optimisation à niveau (5). Cette technique *Marion* s'applique aussi à la sécurité des réseaux (6), mais elle s'adresse surtout au responsable de l'institution et non pas à ceux qui subiraient directement les conséquences du dommage: les patients du SIH n'intéressent pas l'assurance risque de l'entreprise-hôpital. Une telle méthode, grâce à son formalisme rassurant, mais aussi parce qu'elle permet de comparer des niveaux de protection peut être considérée comme une stratégie d'appoint à d'autres stratégies.

La troisième approche est moralisatrice. Elle consiste à édicter une série de règles de conduite pour les utilisateurs du système ou pour ses ennemis potentiels. Le tout assorti de mesures pénales qui se veulent dissuasives. L'apparition de ces règles indique au moins clairement une chose: l'escalade technologique n'est pas appropriée pour assurer la protection absolue des données. La protection d'une banque de données peut donc être comparée à la protection d'une banque tout court: si on y met le prix, on peut toujours réussir une attaque de banque. La question est que, si ce prix est plus élevé que la somme qu'est sensé rapporter le braquage, on travaille à perte. En protection des données, il n'y a pas de protection absolue et ce fait est plutôt rassurant.

L'attaque contre Internet en novembre 1988 a mis en lumière la transformation des ordinateurs en moyens de communication (7). A cette occasion, on a pu lire dans la revue technique la plus en vue des computer scientists une série d'articles qui faisaient tous appel à la conscience morale des professionnels de l'informatique (8, 9, 10). Ceci aurait été impensable il y a dix ans. Encore faudrait-il savoir ce qui doit être protégé et ce qui ne doit pas l'être et cette question n'est malheureusement jamais abordée dans les déclarations morales. En effet la protection des données doit pouvoir être aussi, dans certains cas, la protection contre les données. Mettre sur le même plan la confidentialité d'une donnée sur le cancer d'un patient et les données sur l'utilisation des CFC, c'est inciter à la fraude.

Protection des données et de la sphère privée.

La différence qui existe dans les données d'un SIH et qui mérite qu'on s'engage à le protéger, c'est qu'il s'agit de la protection de la sphère privée. Même dans les scénarios sociaux les plus communautaires, une place existe pour la propriété intime de l'individu (11) et cette *privacy* a une longue histoire qui est antérieure à l'informatique, c'est celle du secret médical.

Une histoire détaillée du secret médical montrerait que celui-ci, après avoir été proclamé par les grecs s'est perdu dans les brumes du moyen âge pour réapparaître au siècle des lumières où il fut déclaré absolu. Son érosion successive par la jurisprudence (obligation de déclarer les maladies contagieuses puis obligation de déclarer les morts suspectes, etc) indique qu'il suit d'assez près l'histoire des rapports de force entre l'autonomie de l'individu et les nécessités sociales.

Mais parmi ceux qui attaquent le secret médical, on retrouve la cohorte des faux amis des patients avec leur double morale: les données ne sont pas soumises à la même protection suivant qu'on se place du point de vue de celui qui collecte les données ou du point de vue de celui sur qui on les collecte. Ceci est particulièrement patent quand un médecin vend sa clientèle avec ses dossiers médicaux.

Sans s'étendre ici sur la perversion de la raison d'Etat invoquée contre les droits de la personne, on retiendra que le secret médical, parce que son principe et son utilité peuvent être compris par tous, est un bon modèle pour les critères qui devraient s'appliquer dans la protection des données du SIH, même si les potentiels attaquants du SIH ne sont pas soumis au secret médical, ni au serment d'Hippocrate.

La question de l'accès limité aux données privées est d'ailleurs depuis toujours en discussion chez tous les informaticiens qui, par leur travail ou leur passion, jouissent d'une facilité d'accès à la *privacy* des gens. On trouva une étonnante réponse à ce problème qand les hackers du MIT définirent leur morale (12) par rapport à l'institution.

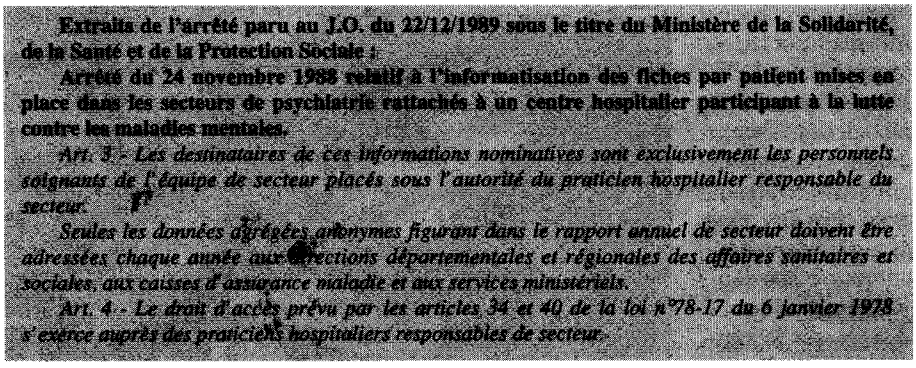
D'ailleurs, le conflit entre raison d'Etat et défense de la "privacy" est plus fondamental et on le retrouve dès le début de l'informatique dans les positions respectives d'un von Neumann et d'un Turing notamment dans leur rapport avec leur employeur, l'Etat. Tant que dura la guerre, ils partagèrent la même morale et tandis que Turing travaillait à la destruction des sous-marins allemands, von Neumann calculait la hauteur optimale pour la bombe d'Hiroshima. Mais, par la suite, les intérêts de von Neumann et de l'Etat se superposèrent encore plus étroitement au moment de la campagne contre Openheimer, alors que ceux de Turing divergeaient toujours plus (13).

Un serment de Turing ?

Ces quelques réflexions essaient de ne pas tomber dans le piège du moralisme qui n'édicte que des règles mais a oublié leur but. En somme ce qu'il faudrait aux données privées, c'est une espèce de Croix-Rouge, un drapeau que l'on puisse hisser sur certains systèmes informatiques en disant : voilà, ici des individus ont déposé leurs affaires personnelles, leur domaine privé, celui qui entre ou qui y sème la pagaille sera dénoncé à l'ensemble de la communauté afin qu'on l'empêche à tout jamais de toucher un terminal.

L'arrêté Brunetière : peut mieux faire !

L'association des *Psychotiques Stabilisés Autonomes** réagit à l'arrêté Brunetière relatif à l'informatisation des fiches par patient dans les secteurs de psychiatrie.



Extraits de l'arrêté paru au J.O. du 22/12/1989 sous le titre du Ministère de la Solidarité, de la Santé et de la Protection Sociale :

Arrêté du 24 novembre 1988 relatif à l'informatisation des fiches par patient mises en place dans les secteurs de psychiatrie rattachés à un centre hospitalier participant à la lutte contre les maladies mentales.

Art. 3 - Les destinataires de ces informations nominatives sont exclusivement les personnels soignants de l'équipe de secteur placés sous l'autorité du praticien hospitalier responsable du secteur.

Seules les données agrégées anonymes figurant dans le rapport annuel de secteur doivent être adressées chaque année aux directions départementales et régionales des affaires sanitaires et sociales, aux caisses d'assurance maladie et aux services ministériels.

Art. 4 - Le droit d'accès prévu par les articles 34 et 40 de la loi n°78-17 du 6 janvier 1978 s'exerce auprès des praticiens hospitaliers responsables de secteur.

Considérant la nature des informations que prévoit l'arrêté du 24/11/1988 en son article 2, après avoir pris acte de l'article 3 de cet arrêté limitant les destinataires de ces informations...

L'association estime qu'il vaut mieux prévenir que réprimer les personnes indélicates. En effet l'occasion de copier un fichier informatique confidentiel peut se présenter et pousser à cet acte délictueux.

Nous préconisons donc afin d'éviter l'hypothèse "paranoïaque" que de telles données nominatives puissent atterrir dans un quelconque cabinet de recrutement :

– que les fichiers réalisés dans les institutions psychiatriques et notamment ceux établis en référence à l'arrêté Brunetière soient déclarés **strictement locaux** aux institutions autorisées à établir de tels fichiers.

– que toute sortie de ces informations de l'institution en ayant effectué la saisie, par quelque moyen que ce soit (papier, télématique...), pour quelque motif que ce soit -y compris technique- (back up), soit déclarée illégale et que des sanctions pénales appropriées soient prévues.

Pour que la présence des données de tels fichiers hors des institutions les ayant saisies devienne en soi illégale, l'association considère que la maintenance informatique doit être locale, effectuée sur place et que les personnes autorisées à accéder à ces informations ne l'effectuent que par le mode de la **consultation** sans aucun droit de **duplication** de quelque fiche que ce soit (réserve faite d'une copie demandée explicitement par l'intéressé lui-même pour communication au médecin de son choix).

■

Loïc Le Goff

**** Psychotiques Stabilisés Autonomes, Boite Postale 603 75826 PARIS CEDEX 17 Tél. : 42.28.04.48.***

Ce qui compte, c'est de savoir ce que l'on protège. Et si ce qu'on protège a un sens, on trouve une motivation et un code déontologique. Car la valeur intrinsèque d'un travail, ne garantit pas son sens et son humanisation ne garantit point celle des finalités qu'il sert (14).

Alain Turing, avant de se suicider en mordant dans une pomme au cyanure comme Blanche Neige a vu passer tous les sales petits nains de l'informatique et il a pris son parti. Il fut le premier hacker en s'attaquant au code d'Enigma. Sa vie durant, il sut garder les secrets qu'on lui confia. Mais il fut aussi le premier à se ranger du côté de la désobéissance civile lorsque la raison d'Etat voulut instrumentaliser son savoir. Pourquoi les informaticiens plutôt que le serment d'Hipocrate ne feraient-il pas le serment de Turing?

■

— Références —

(1) *Claude Got, Rapport sur le Sida, Projet de loi relatif à l'enregistrement et au traitement manuel ou automatisé de données nominatives de santé à des fins de recherche médicale, Flammarion 1989 p 338-340*

(2) *Patrice Degoulet Les Systèmes d'Information Hospitaliers: Stratégies et Perspectives... p. 288-298*

(3) *D. de Roulet, A. Rouge et al, Strategies for an operating environment in a Distributed Hospital Information System, in: Medinfo 1989, Singapour*

(4) *Jean-Pierre Cahier, Dossier virus, Petits monstres, in Terminal, juin 1989, P. 19.*

(5) *J.M. Lamère, La sécurité informatique: approche méthodologique Editions Dunod 1985 ISBN 2-04-01-6503-7*

(6) *J.M. Lamère La sécurité des réseaux Editions Dunod informatique 1987 2-04-016911-3*

(7) *Winograd, T and Flores F. Understanding computer and Cognition, a new foundation for design (Addisson Wesley Publishing Company Inc 1988)*

(8) *Computer professionals for Social Responsability, CPSR Statement on the Computer Virus in Communications of the ACM June 1989 p 699*

(9) *Jerome H. Saltzer, Teaching Students About Responsible Use of Computers, in: Communications of the ACM June 1989 p 704*

(10) *Vint Cerf, Ethics and the Internet, in: Communications of the ACM, June 1989 p 710*

(11) *P.M., Bolo-bolo, version anglaise...*

(12) *Steven Levy, Hackers, heroes of the computer revolution, Chap 3. The Hacker Ethic, p 26-36, Anchor Press/Doubleday, New-York 1984, ISBN 0-385-19195-2*

(13) *Andrew Hodges, Alan Turing: the Enigma of intelligence, Hutchinson Publishing Group 1983 en français : ISBN 2-228-88081-7*

(14) *André Gorz, Métamorphoses du travail, quête du sens, Editions Galilée, 1988*