CHAPITRE 1

La protection des données personnelles à la croisée des chemins

Michel GENTOT

Evoquer l'expérience française en matière de protection des données personnelles, c'est, plus encore que de rendre compte de 20 années de doctrine ou s'efforcer à l'exercice du "bilan", mettre en lumière les enjeux liés à la prochaine modification de la loi du 6 janvier 1978 que dicte la transposition de la directive européenne du 24 octobre 1995.

Dès 1973, la Suède avait ouvert la voie en se dotant d'une loi protégeant les personnes contre un usage abusif de l'informatique. Le Land de Hesse, en Allemagne, avait suivi, précédant de peu la France. Ces lois, et — pourquoi ne pas le reconnaître, la loi française — ont inspiré la première convention internationale sur le sujet : la Convention du 28 janvier 1981 du Conseil de l'Europe, dite "convention 108". Cette convention, qui est "la sœur cadette" de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, est aujourd'hui ratifiée par vingt Etats. Très au-delà de l'Europe, des pays aussi différents que le Canada, Singapour, l'Australie, la Nouvelle-Zélande, Hong Kong, le Japon, Israël, se sont également dotés de lois "informatique et libertés", même si leur champ d'application est le plus souvent limité aux seuls fichiers publics. Enfin, il est frappant de constater l'impatience qu'ont manifestée nos voisins du Centre et de l'Est européen à se doter de telles lois en signe d'affranchissement du joug des années noires : République Tchèque (1992), Lituanie (1996), Pologne et Hongrie (1997), Lettonie (1998). Ni la Russie, ni la Roumanie ne manquent à l'appel. On doit se réjouir de cette liberté qui essaime.

La loi française "informatique et libertés" a un peu plus de vingt ans et, sans doute, les développements techniques imposent-ils de l'adapter sur plusieurs points.

Ainsi, l'obligation de soumettre à examen préalable de la CNIL toute création de fichier informatique, quelle qu'en soit son importance ou ses incidences, est devenue assez largement vaine à l'heure de la micro-informatique et d'Internet, qui permet à chacun d'entre nous de créer une page personnelle accessible au monde.

De même, la disparité des pouvoirs de contrôle de la CNIL selon la nature publique ou privée des fichiers, qui avait son sens il y a vingt ans lorsque l'informatique était d'abord un outil mis en oeuvre par l'administration ne se justifie plus**.** Un fichier de gestion des concessions de cimetières ou le fichier du personnel d'une école primaire soulève sans doute moins de difficultés qu'un fichier de souscripteurs d'assurance-vie, les logiciels "de score" des établissements de crédit ou un registre épidémiologique de séropositivité au VIH.

Mais l'essentiel n'est pas là. Si le développement des nouvelles techniques et l'internationalisation des échanges ont incontestablement contribué à faire partager des préoccupations qui, il y vingt ans encore, passaient pour relever d'une exception française, on peut se demander si cette généralisation, voire cette universalisation, n'a pas modifié la nature des garanties que nous avons, depuis les origines, considérées comme essentielles. Lorsque nous évoquons la protection des données personnelles ou de la vie privée, sommes-nous toujours sûrs de nous situer sur le terrain que le législateur français de 1978 avait ainsi balisé dans l'article premier de la loi : "*L'informatique ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques*" ? Une telle proclamation d'il y a vingt ans a-t-elle encore un sens ?

Il n'est pas anormal que la Commission nationale de l'informatique et des libertés essaye de répondre à ces questions, tant elle est mêlée, et depuis si longtemps, aux évolutions législatives et techniques, dans ce domaine.

LA "MARCHANDISATION" DES DONNÉES PERSONNELLES

Il y a vingt ans, les informations nominatives étaient essentiellement des renseignements d'ordre administratif, policier, politique ou fiscal et la protection instituée au bénéfice des citoyens à l'égard du traitement automatisé de ces informations procédait de la volonté de protéger le citoyen contre "l'Etat Léviathan", ou plutôt son autre face, "l'Etat Safari" si l'on se réfère au projet imaginé par l'administration en 1974 consistant à interconnecter l'ensemble des fichiers publics grâce au numéro de sécurité sociale. C'est la révélation de ce projet qui devait d'ailleurs aboutir quelques années plus tard à l'adoption de la loi du 6 janvier 1978. C'est ce projet qui explique encore les réserves de la Commission à l'égard de tout usage généralisé de ce numéro.

Cependant, en vingt ans, l'information nominative a acquis une valeur marchande. Cet attrait commercial s'est très tôt manifesté dans le domaine de la prospection commerciale. Une adresse peut révéler une situation économique et sociale, un prénom, un âge ou un profil. En outre, les possibilités nouvelles de corrélation associées à l'outil statistique et au développement des logiciels de

"fouille" des données (*data mining*) permettent de faire produire à une information de base, somme toute assez ordinaire, beaucoup plus de renseignements qu'on ne l'imaginerait.

Cette valorisation économique des données personnelles explique l'attrait nouveau que recèlent les données publiques : un nom et une adresse accessibles au public, ce sont aussi un nom et une adresse que les opérateurs commerciaux souhaiteront utiliser à des fins commerciales. L'utilisation à cette fin en Allemagne ou en France des annuaires du téléphone ou en Grande-Bretagne ou en Espagne, des listes électorales, le manifestent avec éclat.

Cet attrait commercial peut parfois se nicher dans les informations les plus insoupçonnées. Ainsi, en France, les bans de mariage publiés à la porte des mairies pendant les quinze jours qui précèdent l'union sont devenus une précieuse matière première pour les opérateurs commerciaux. On est pourtant loin des justifications initiales de la publication des bans. Le droit canon était soucieux d'éviter la pratique médiévale du mariage "*in facie ecclesiae*" par lesquels les époux venaient déclarer clandestinement leur union à la porte de l'église pour échapper à une éventuelle opposition des familles. Sur ce point, l'Etat laïque, en maintenant le principe de cet affichage, a tenu la main au droit canon sans que quiconque ait pu songer que les opérateurs commerciaux feraient leur miel de cette procédure d'opposition à mariage.

Cette tendance à la "marchandisation des données" s'est accrue avec la crise de la consommation de masse. Jadis, l'action commerciale consistait, pour l'essentiel, à présenter une offre généraliste: il suffisait de disposer d'un nom et d'une adresse pour envoyer un document de prospection identique à un très grand nombre de personnes. Désormais, l'offre s'individualise et on est passé au "sur mesure" de la prospection commerciale ; c'est ce que les professionnels appellent la technique du "*one to one*" ou désormais la "CRM" pour "*customer relationship management*". Une meilleure connaissance du consommateur, de ses goûts, de ses habitudes est recherchée qui permettra de cibler beaucoup plus précisément l'action commerciale à entreprendre. Cette tendance trouvera son accomplissement dans le monde virtuel d'Internet qui constitue un gisement de données sur nos comportements et nos centres d'intérêts que des outils nouveaux, sophistiqués et disponibles permettent désormais de collecter, trier, classer, en un mot, d'exploiter. Ce faisant, la collecte des données personnelles et leur enrichissement deviennent de véritables armes aux mains d'entreprises qui se livrent à une concurrence sans merci.

Une des questions les plus aiguës en matière de protection des données personnelles est d'ailleurs celle du sort des fichiers de clientèle en cas de fusion, de concentration ou d'absorption d'entreprises, notamment dans le monde d'Internet où certaines entreprises ne se créent que dans le souci de constituer un fichier nominatif de visiteurs du site ou de clients internautes, la réalité de leur activité commerciale se résumant, bien souvent, à l'ouverture d'un site et à la collecte de données personnelles à revendre.

Les conséquences d'une telle marchandisation des données personnelles sont considérables, et n'ont peut-être pas fini de se déployer, dans les registres les plus divers. En premier lieu, c'est cette tendance qui a permis, non sans paradoxe, à l'Union européenne et, bien au-delà d'elle, à des Etats de plus en plus nombreux de s'accorder sur une réglementation commune en matière de protection des données personnelles. Cette évolution doit conduire, en deuxième lieu, à s'interroger sur la nature de l'autorité de contrôle. Elle explique, enfin, une certaine forme de "contractualisation" de la protection des données personnelles, qui appelle à une grande vigilance.

La "marchandisation" des données personnelles, à l'origine de l'internationalisation des principes de protection ?

L'élaboration à partir de 1990 d'une directive européenne en matière de protection des données personnelles avait pu susciter certaines inquiétudes. La CNIL l'avait écrit crûment dans un de ses rapports d'activité : "Veut-on l'Europe des marchands ou celle des droits de l'Homme ?" Et, c'est bien au motif que les données personnelles ont été considérées comme étant aussi des marchandises que l'Union européenne a pu intervenir sur ce sujet. Le fondement juridique de la directive du 24 octobre 1995 est l'article 100A du traité de Maastricht relatif à la liberté de circulation des marchandises, services et capitaux. L'article premier § 2 de la directive européenne ne laisse guère planer de doute sur le sujet : "Les Etats-membres ne peuvent restreindre ni interdire la libre circulation des données à caractère personnel entre Etats-membres pour des raisons relatives à la protection [des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel]".

Plusieurs facteurs ont cependant apaisé les inquiétudes initiales.

En premier lieu, la directive a offert le considérable avantage de doter l'Union européenne d'un socle commun de garanties et de protections très largement inspirées des principes généraux de la législation française de 1978 (principe de finalité, pertinence des données traitées, durée de conservation limitée, droit d'accès, droit d'opposition, etc). Les rédacteurs de la directive ont d'ailleurs pris soin d'évoquer à plusieurs reprises "les droits fondamentaux reconnus dans les constitutions et les lois des Etats-membres", la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, et tout particulièrement son article 8, pour préciser que "le rapprochement de ces législations ne devait pas conduire à affaiblir la protection qu'elles assurent mais devait, au contraire, avoir pour objectif de garantir un niveau élevé de protection dans la communauté".

Au-delà de ces affirmations de principe et en deuxième lieu, la directive du 24 octobre 1995 a institué un mécanisme de coopération entre autorités de

contrôle des Etats-membres qui se réunissent régulièrement (au moins une fois par mois) pour partager leurs expériences, harmoniser leurs recommandations et rendre des avis, à la demande de la commission européenne, sur tous les sujets touchant à la protection des données personnelles. Ce groupe des commissaires européens à la protection des données, que l'on nomme communément "groupe de l'article 29" accomplit un travail considérable et a rendu plusieurs avis ou recommandations qui permettent à ces autorités de parler d'une même voix. Il en fut ainsi sur la durée de conservation des données de connexion à Internet, sur les mentions d'informations devant figurer sur les sites web, sur l'exploitation des données publiques ou encore sur le publipostage électronique. Ces avis ont été, à bien des égards, déterminants lors de l'élaboration de directives spécifiques ou de l'adoption de législations nationales sur ces sujets.

Enfin, les dispositions particulières retenues par la directive du 24 octobre 1995 en matière de flux transfrontières de données personnelles constituent un puissant levier de protection des données dans le monde. En effet, la directive européenne subordonne, dans son principe, les transferts de données vers les pays tiers à l'exigence d'un niveau de protection adéquat, que ce dernier résulte d'une loi, d'un mécanisme d'autorégulation ou d'un contrat de protection des données passé entre l'entreprise expéditrice et l'entreprise destinataire établie hors d'Europe. Elle attribue à la commission européenne un pouvoir d'appréciation de la protection offerte et lui reconnaît un pouvoir de négociation avec ceux des Etats ne satisfaisant pas à ce niveau d'exigence.

Les longues discussions entreprises entre la commission européenne et les Etats-Unis, qui se sont conclues par les accords dits de "*Safe harbor*", auront eu, bien au-delà du nombre encore faible d'entreprises américaines ayant souscrit à ces engagements, une influence tout à fait déterminante. Certes, le développement des usages "grand public" et commerciaux d'Internet, ainsi que les préoccupations exprimées par les consommateurs et les internautes dans des termes semblables de part et d'autre de l'Atlantique y auront également contribué. Selon le Financial Times, trois cents propositions de lois dans les Etats américains et près d'une douzaine au niveau fédéral ont été déposées dans le souci d'assurer une protection aux données personnelles.

On apprenait également récemment que la justice américaine, refusant de considérer un fichier de clients d'une société en faillite comme un élément de patrimoine, s'était opposée à la commercialisation des données personnelle qui y étaient conservées. La Cour des faillites de Boston a considéré, dans le cas d'espèce où il s'agissait d'un site web de vente de jouets, que la loi américaine de 1998 sur la protection en ligne de la vie privée des enfants s'opposait à une telle vente de coordonnées d'enfants, et surtout, que les personnes concernées n'ayant pas été informées lors de leur connexion à ce site d'une éventuelle cession de leurs données à des tiers, la vente du fichier aurait constitué un délit de pratique déloyale.

Enfin, au-delà des Etats-Unis, certains Etats se sont dotés récemment d'une loi de protection des données personnelles applicables au secteur privé - tel est le cas de l'Argentine - quand d'autres ont étendu l'application de leur loi, jusqu'alors cantonnée au seul secteur public, aux activités marchandes. Tel est le cas de la loi canadienne sur la protection des renseignements personnels et les documents électroniques qui, adoptée le 13 avril 2000, est entrée en vigueur le 1er janvier 2001 et de la loi australienne qui a été amendée en ce sens en décembre 2000 pour entrer en vigueur le 1er décembre 2001.

Ainsi, ce qu'il est convenu d'appeler la "mondialisation" a pu contribuer, en attachant des droits particuliers aux données personnelles considérées comme une marchandise appelée à circuler, à élargir considérablement le périmètre géographique de la protection. C'est sans doute la première conséquence, et une des plus heureuses autant qu'inattendues, de la "marchandisation" de nos données personnelles.

Vers une modification de la nature de l'autorité de contrôle ?

Ce même mouvement aboutit, par l'effet combiné des évolutions industrielles et commerciales, à mettre en question la nature de l'autorité de contrôle. Celle-ci, initialement très clairement située sur le terrain des libertés publiques a désormais, au moins pour partie, un rôle de régulation des marchés. Il n'est pas contestable, en tout cas, que les interventions de la CNIL ont de plus en plus souvent des incidences, qui peuvent être considérables, sur les intérêts commerciaux.

Cet élément nouveau peut conduire à préconiser la présence de professionnels au sein de ces autorités administratives indépendantes. Il est en effet généralement soutenu que la participation de professionnels au sein de l'autorité de contrôle serait de nature à susciter davantage l'adhésion des entreprises concernées, à assurer une meilleure information des acteurs économiques et à permettre de réagir plus rapidement et avec plus de souplesse aux évolutions. Cela vaudrait aussi bien pour la détermination de la "règle du jeu" que pour le prononcé d'éventuelles sanctions.

Cependant, cette légitime présence des professionnels au sein de l'autorité de contrôle pourrait connaître certaines limites.

La première limite tient à l'indépendance: comment concilier la présence de professionnels et l'indépendance à l'égard des marchés ? Ce problème a toujours été posé, même aux Etats-Unis où, dans les années 80, certaines *independant regulatory commissions* ont été mises en sommeil parce que l'on redoutait leur capture par les entreprises. Ce délicat problème peut être résolu par le biais d'incompatibilités légales qui interdisent aux membres des autorités

administratives indépendantes d'avoir des intérêts dans le secteur qu'elles contrôlent ou de règles déontologiques interdisant pendant un certain temps aux membres de ces autorités de retourner dans les entreprises qui relevaient de leur contrôle. Encore convient-il que ces incompatibilités soient énoncées en termes nuancés.

La loi du 6 janvier 1978 offre à cet égard une assez jolie illustration de la complexité du problème. L'article 8 de la loi du 6 janvier prévoit que la qualité de membre de la CNIL est incompatible avec l'exercice de fonctions ou la détention de participations dans les entreprises concourant à la fabrication de matériels utilisés en informatique ou en télécommunications ou à la fourniture de services dans ces domaines. Comment peut-on faire une plus grande place aux professionnels et maintenir une incompatibilité rédigée en des termes si généraux ? Comment garantir, sinon l'indépendance du moins l'impartialité des membres de la Commission, en revenant sur cette incompatibilité ? C'est une des difficultés qu'aura à résoudre en France la future loi de transposition de la directive européenne.

La deuxième limite tient à ce que l'on pourrait appeler une certaine "judiciarisation" de l'autorité de contrôle. Les enjeux en termes financiers des décisions prises peuvent être tout à fait considérables; aussi les décisions de l'autorité de contrôle sont-elles de plus en plus fréquemment contestées devant le juge, mouvement qui ne peut qu'être appelé à s'amplifier si la CNIL devait se voir reconnaître un véritable pouvoir de sanction administrative et, tout particulièrement, le pouvoir d'infliger des sanctions pécuniaires. D'ores et déjà, les derniers avertissements qu'a délivrés la CNIL ont tous fait l'objet d'un recours devant le Conseil d'Etat.

En définitive, l'autorité de contrôle doit veiller avec une plus grande rigueur au respect de formalités de plus en plus nombreuses, tant à l'occasion de l'élaboration des normes que lors du prononcé de sanctions. Il en résulte un formalisme nouveau qui doit être scrupuleusement respecté si l'on souhaite éviter une annulation au contentieux. Aussi, peut-on se demander s'il n'y a pas une certaine contradiction entre les objectifs ayant présidé à la création des autorités (grande souplesse d'intervention, plus grande légitimité attendue de la présence des professionnels) et les exigences nouvelles qu'impose une éventualité plus grande de contentieux, au risque de voir mise en cause la présence de professionnels dans les formations spécialisées chargées de sanctionner les comportements illicites.

En tout état de cause, le risque existe que les enjeux économiques ou financiers de ces interventions ne cessant de croître, la priorité soit donnée à cette mission nouvelle de régulation d'un marché, l'autorité pouvant alors être contrainte à déserter le terrain des libertés individuelles ou publiques, qui était celui de ses origines, pour se transformer en "luxueux" corps de contrôle spécialisé.

Vers une "contractualisation" de la protection des données personnelles ?

C'est une troisième conséquence possible de la "marchandisation" des données personnelles.

Il est frappant de constater que la directive européenne du 24 octobre 1995 relative à la protection des données à caractère personnel et à la libre circulation de ces données fait du "consentement" une garantie essentielle de protection des données personnelles jusqu'à le viser au titre des principes de légitimité des traitements. Or, la loi française du 6 janvier 1978 ne fait qu'une place tout à fait résiduelle à cette notion. Une seule disposition de notre loi retient le consentement, s'agissant des données particulièrement sensibles (origines raciales, appartenances politiques, syndicales, religieuses, philosophiques, mœurs) qui ne peuvent être collectées et traitées, sauf dérogation exceptionnelle, qu'avec le consentement exprès des personnes concernées. Plus récemment, l'obligation du consentement a été introduite en droit français pour certains traitements de recherche lorsqu'ils font appel à un "prélèvement biologique identifiant" ou à un "acte invasif" (en pratique, lorsqu'il s'agit de recherche génétique ou d'une prise de sang effectuée dans le cadre d'un essai clinique).

L'absence de cette notion de consentement dans la loi française "informatique et libertés" est d'autant plus frappante qu'en droit français l'exigence du consentement est un véritable "verrou" protégeant la vie privée. On trouve cette notion dans le code civil (c'est le droit à l'image), dans le code pénal (qui interdit les écoutes téléphoniques ou les enregistrements de conversation sans le consentement des personnes concernées, ou la prise de photographies d'une personne dans un lieu privé sans le consentement de celle-ci) ou encore dans le code de procédure pénale (les perquisitions ou les saisies ne peuvent être opérées durant l'enquête préliminaire au domicile d'une personne, sauf consentement exprès de celle-ci). Les exemples pourraient être multipliés.

On devrait dès lors s'attendre à ce que cette notion figure en bonne place dans la loi de protection des données personnelles ; et pourtant elle y est absente, sous quelques réserves résiduelles.

Cela signifie sans doute qu'en adoptant la loi de 1978, le législateur a pensé que le traitement de nos données personnelles excédait très largement le seul registre de la protection de la vie privée et touchait aux fondements mêmes de l'Etat de droit. Le citoyen ne peut pas "consentir" à un amoindrissement des garanties qui lui sont reconnues par l'Etat de droit, c'est-à-dire par le contrat social qui le fonde.

Mais il en va tout autrement, bien sûr, si, sous l'influence de la "marchandisation" des données personnelles, on en vient à considérer que la protection des données relève du contrat liant un consommateur à une entreprise, autour du principe général du droit privé qu'est la loyauté ou la bonne

foi devant présider aux conventions légalement passées entre les parties. L'approche américaine de la protection des données personnelles qui s'articule autour du "notice and choice" laissant chacun libre d'accepter ou de refuser que ses données soient traitées et mettant particulièrement en valeur l'information préalable et la "confiance" réciproque entre "partenaires" s'inspire de cette philosophie qui est loin d'être absente de la réglementation européenne et qu'illustrent des pratiques professionnelles toujours plus nombreuses.

Consentir à quoi ?

C'est très certainement la question qui appelle à notre plus grande vigilance. A quoi servirait-il de poser comme une garantie l'exigence du consentement si, en pratique, les personnes ne savent pas parfaitement à quoi elles consentent ? Or, bien souvent, la crainte qu'une parfaite information ne conduise les personnes à refuser de consentir ou une certaine approche commerciale du problème peuvent contribuer à dégrader l'exigence du consentement.

Ainsi, la directive européenne prévoit, s'agissant des flux transfrontières de données, que par dérogation avec le principe posé d'un niveau de protection adéquat, le transfert de données peut avoir lieu si la personne concernée a "*indubitablement donné son consentement au transfert envisagé*". Que signifie en pratique une telle prescription ? Le consentement doit-il être considéré comme acquis lorsque la personne concernée a été informée de la finalité de ce transfert et de sa destination (les Etats-Unis par exemple) ou bien alors cette exigence doit-elle conduire à ce que la personne soit précisément informée, non seulement que ses données vont être transférées aux Etats-Unis, mais aussi qu'aucune règle de protection des données personnelles ne la garantit efficacement contre un usage abusif de ses données personnelles une fois exportées ? On sent bien que dans l'une et l'autre de ces hypothèses, le consentement n'aura pas la même portée et surtout que la réponse ne sera pas la même.

Pour prendre un autre exemple, la CNIL a été confrontée, à la pratique de certains opérateurs qui constituent des "mégabases de données " à des fins de prospection et d'exploitation commerciales. Ces opérateurs distribuent à des millions d'exemplaires des questionnaires sur nos comportements d'achat, nos loisirs, nos goûts, comportant plusieurs centaines de questions.

Ces questionnaires sont distribués gratuitement, ils précisent que les réponses sont facultatives et comportent une mention destinée à autoriser la cession de données à des tiers ainsi rédigée "*Je souhaite recevoir des bons de réduction ou des cadeaux de vos partenaires commerciaux par votre intermédiaire*". Une telle formule valait-elle consentement ? En "consentant" à recevoir des cadeaux, les personnes concernées avaient-elles pleinement conscience que leurs données allaient être cédées, exploitées, profilées, parfois

par leur propre banque (connue de l'opérateur ayant collecté les données parce qu'il posait précisément une question à ce sujet, ou par leur opérateur de télécommunications etc.) ?

La CNIL est bien évidemment intervenue pour rendre ces mentions d'information plus explicites de sorte que les personnes qui répondent à ces questionnaires dans le seul but d'obtenir des offres ou autres avantages financiers soient pleinement conscientes, qu'en le faisant, elles alimentaient des bases de données comportementales appelées à être commercialisées. D'ailleurs les opérateurs en cause se sont dotés, à la suite des interventions de la CNIL, d'un "code de déontologie et de bonnes pratiques" qui a notablement amélioré l'information des personnes.

Consentir comment ?

C'est la deuxième question qui pose à la fois un problème de loyauté et un problème de preuve.

La loyauté est en cause, lorsque nous voyons apparaître fréquemment des cases déjà cochées sur des formulaires de collecte d'informations tout particulièrement sur Internet, assorties d'une formule du type "*J'accepte que mes données soient transmises à des tiers*". De telles pratiques, hélas assez répandues, paraissent tout à fait déloyales.

Mais c'est aussi la preuve du consentement qui peut poser problème : comment un responsable de traitement peut-il rapporter la preuve que la personne concernée a bien consenti à ce que ses données soient traitées ou cédées ?

En France quand il y a exigence de consentement, la loi précise le plus souvent que ce consentement doit être "exprès", ce qui a été considéré, notamment par le Conseil d'Etat, comme signifiant que ce consentement devait être écrit. Evidemment, sur Internet, la chose est sans doute plus délicate, et un "double click" peut être envisagé manifestant, par le premier "click", que la personne a été informée de ses droits et, par le deuxième "click", qu'elle a consenti en toute connaissance de cause.

Ce souci de la preuve peut d'ailleurs conduire, en pratique, à produire un écrit là où pourtant le consentement exprès n'est pas exigé. Tel est le cas, en particulier dans le domaine de la recherche médicale qui, pourtant, n'exige le consentement que dans deux situations précises (lorsqu'il y a prélèvement invasif ou prélèvement biologique identifiant) et non pas dans toutes. C'est ainsi que des documents d'information sont le plus souvent remis au patient et restitués au

médecin, signés par l'intéressé, pour attester que sa participation à l'étude ou à la recherche médicale est tout à fait volontaire.

Mais, il faut bien être conscient qu'un tel formalisme n'est pas toujours synonyme de garantie.

Ainsi pour n'évoquer qu'un exemple, la CNIL a récemment été saisie par les parents d'un enfant atteint d'un cancer qui s'étaient vu remettre un document les informant que le cas médical de leur enfant allait contribuer à une recherche sur la maladie particulière dont il était atteint et leur demandant leur consentement à cette fin. Le document était si peu explicite que les parents concernés, pourtant très certainement ouverts à une telle possibilité, n'ont retenu qu'une chose : que l'on tentait de leur extorquer leur consentement alors qu'on ne leur en précisait ni la portée ni les conséquences.

Il est vrai que, dans ce domaine, la signature exigée des personnes pour preuve de leur consentement est souvent utilisée pour éviter la mise en cause de la responsabilité du médecin et peut s'apparenter quelquefois à un blanc-seing, voire même à une "réquisition", bien éloignée de ce que suppose l'exigence d'un consentement libre et éclairé.

Consentement et liberté de ne pas consentir

En théorie, le consentement ne peut se concevoir que s'il y a liberté de ne pas consentir. Tel est le cas par exemple en matière de prospection par automate d'appel, par télécopie (depuis la directive du 15 décembre 1997 relative à la protection des données personnelles et de la vie privée dans le secteur des télécommunications) et par prospection électronique à partir des mails capturés sur les espaces publics de l'Internet. Dans ce cas, on est libre de consentir ou non, et si l'on ne consent pas, l'emploi de ces moyens doit être exclu. Dans le souci de rendre plus effectives encore ces garanties, la CNIL a saisi l'occasion de l'examen d'un projet de loi sur la société de l'information, qui évoquait notamment le problème de la prospection électronique non sollicitée, pour proposer au Gouvernement de prévoir une sanction particulière et adaptée à Internet consistant à punir d'une amende par adresse toute collecte de mails à des fins de prospection commerciale opérée dans les espaces publics de l'Internet (forums de discussion, listes de diffusion, etc.).

Cependant dans bien des cas, il y a "consentement"sans liberté de consentir.

Ainsi, par exemple en matière de fichiers centraux d'impayés et tout particulièrement en matière de crédit à la consommation. Lorsque le service sollicité par le consommateur (l'ouverture d'une ligne de téléphone mobile, une location de voiture, un crédit à la consommation) ne lui est offert que s'il donne

son accord pour que les informations le concernant soient enregistrées dans un fichier central accessible à l'ensemble des professionnels du secteur concerné, le consommateur est-il vraiment libre de refuser de consentir à une telle divulgation de ses données à des tiers ? A-t-il un autre choix ? En France, sur ce point, le principe du secret bancaire interdit la constitution de fichiers positifs et n'autorise que la mise en place de fichiers dits "négatifs", c'est-à-dire d'impayés. Mais il a fallu une loi pour mettre en place ces fichiers négatifs, tout au moins en matière bancaire.

La Commission a été récemment saisie d'une plainte qui illustre le problème du "consentement" sans liberté de consentir. La filiale française d'une entreprise américaine a exigé de l'ensemble de ses salariés qu'ils "consentent" au transfert des données de gestion du personnel aux Etats-Unis, sur le fondement de la directive du 24 octobre 1995, au titre des dérogations, et dans le souci de se dispenser d'élaborer un contrat de flux transfrontières de données. Les salariés ont-ils le choix de ne pas consentir ? Évidemment non, malgré le courage de celui qui a saisi la CNIL sur le sujet.

On relèvera en outre qu'en procédant ainsi, l'entreprise tentait de se soustraire à l'obligation faite par la directive européenne d'assurer aux données personnelles transférées un niveau de protection adéquat.

Enfin, et plus généralement, il convient de souligner que les opérateurs les plus cyniques prétendent que l'exigence du consentement ne leur pose aucun problème : lorsqu'elle est imposée, ils s'y plient en suscitant les consentements par des offres diverses d'avantages plus ou moins chimériques, mais généralement peu coûteux pour eux : c'est alors un peu la liberté de ne pas consentir que l'on achète !

C'est la raison pour laquelle, dans plusieurs domaines, la loi française pose de véritables interdictions de sorte que le "consentement" ne puisse pas autoriser des pratiques qui paraissent contraires à nos principes généraux.

C'est notamment le cas en matière d'exploitation à des fins commerciales des données relatives aux prescriptions médicales. Si de telles informations peuvent être exploitées sous forme statistique par des opérateurs privés (laboratoires de recherche médicale notamment), le code de la santé publique, à la suite d'une proposition de la CNIL, pose clairement le principe d'une interdiction d'exploitation commerciale de ces données lorsqu'elle sont associées à l'identité du médecin prescripteur. Cette interdiction a été faite à un moment où des sociétés privées de plus en plus nombreuses proposaient aux médecins de ville ou aux pharmacies d'assurer gratuitement l'informatisation de leur cabinet ou de leur officine en contrepartie d'une connaissance exhaustive des prescriptions de médicaments.

Plus récemment la CNIL a saisi le ministre de la Santé en demandant que le même principe d'interdiction d'exploitation commerciale des données soit posé

pour les données de santé sur Internet qui ne sauraient, en aucun cas, devoir être considérées comme de vulgaires "marchandises".

C'est un même souci de préserver certains de nos faits et gestes de cette tendance à la "marchandisation" qui a conduit la CNIL, en liaison avec l'ensemble de ses partenaires européens, à proscrire toute collecte à l'insu des personnes concernées, et le plus souvent à des fins d'exploitation commerciale, d'adresses e-mail depuis les espaces publics de l'Internet tels que des forums de discussion ou des listes de diffusion : on peut souhaiter dialoguer entre internautes sur un même thème d'intérêt général et ne pas souhaiter se sentir épié par la convoitise commerciale.

Ces quelques exemples manifestent sans doute les limites de la "contractualisation" de la protection des données personnelles et nous invitent à revenir sur les origines de nos législations de protection des données.

UN RETOUR AUX ORIGINES : LA SAUVEGARDE DE LA LIBERTÉ INDIVIDUELLE

En subordonnant le traitement d'informations nominatives au principe de finalité (quelles données collectées et traitées et à quelles fins ?), en limitant la durée de conservation de ces données à ce que justifie la finalité des traitements en cause, en exigeant que les données conservées soient "pertinentes" et non "excessives" au regard de la finalité de la collecte et en imposant des mesures générales d'information des citoyens sur ces différents points, les lois de protection des données personnelles et de la vie privée ont décliné, à l'aube de la société de l'information, les principes fondamentaux de proportionnalité et de retenue qui avaient précédemment et successivement conduit l'Etat à s'interdire, par exemple, d'opérer des perquisitions de nuit au domicile d'un particulier, de saisir des objets ou des effets lui appartenant en enquête préliminaire sans son consentement exprès ou encore de le placer sous écoute téléphonique hors un cadre juridique rigoureux et dans certaines circonstances d'une gravité particulière dont l'appréciation est soumise au contrôle d'une autorité indépendante (l'autorité judiciaire pour les écoutes judiciaires, une autorité administrative indépendante pour les interceptions de sécurité).

Ces principes de protection des données personnelles n'ont nullement eu pour effet de priver la police des moyens d'action dans la mesure où, tout au contraire, ces derniers se sont développés, quasi mécaniquement, au fur et à mesure de l'informatisation de nos sociétés. C'est précisément la raison pour laquelle le législateur a souhaité définir, dès les premiers balbutiements de la société numérique, des garanties destinées à prévenir toute rupture de l'équilibre

entre les droits du citoyen et les prérogatives de l'Etat. Ces garanties s'articulent autour de trois idées : principe de proportionnalité, souci de la personne humaine, droit à l'oubli.

Le principe de proportionnalité

Un exemple l'illustre. Un collège du Sud de la France a saisi la CNIL d'un projet de contrôle d'accès à la cantine scolaire reposant sur l'enregistrement des empreintes digitales des élèves. Environ 350 personnes étaient concernées par le traitement qui comportait deux bases de données, gérées de manière distincte : un fichier de gestion exploité par le service de l'intendance pour la facturation, une base de données biométriques comportant une représentation codée des empreintes digitales de chaque personne.

L'administration du collège faisait valoir que l'utilisation du système permettait de supprimer toute manipulation d'argent à l'intérieur de l'établissement, et de ne plus gérer les problèmes de cartes oubliées, perdues ou volées qui alourdissaient les tâches de gestion. Il était également avancé que toutes les tentatives de fraude, certains collégiens tentant de manger deux fois, seraient mises en échec par le système !

La Commission a rendu un avis défavorable au motif que le traitement était excessif au regard de la finalité poursuivie. En effet, si la constitution des bases de données d'empreintes digitales peut être justifiée dans certaines circonstances particulières où l'exigence de sécurité et d'identification des personnes est impérieuse, la CNIL demeure réservée à l'égard de la généralisation de telles bases de données dans la mesure où, compte tenu des caractéristiques propres aux empreintes digitales, elles sont susceptibles d'être utilisées à des fins tout à fait étrangères à leur finalité initiale. En effet, à la différence d'autres données biométriques, telles que le contour de la main, l'iris ou la reconnaissance vocale, les empreintes digitales sont liées à chacun de nos gestes les plus quotidiens et peuvent être exploitées à des fins d'identification et de recherche des personnes. En devant montrer "patte blanche" pour accéder à la cantine, ce sont des stocks de preuves qui auraient pu se constituer, collège après collège, faisant de tous les enfants en âge scolaire des suspects potentiels de toutes les infractions à venir.

Ce principe de proportionnalité est d'autant plus essentiel que la constitution d'un fichier qui résultait jadis d'une volonté, d'un choix de l'administration ou d'une entreprise (nous étions fichés parce que quelqu'un souhaitait nous ficher) peut désormais résulter de la seule technique.

Un appel passé depuis un téléphone portable permet aux opérateurs de télécommunications sinon de nous suivre à la trace, du moins de pouvoir identifier à quelques centaines de mètres près - zone de couverture de la cellule

radio - le lieu où nous nous trouvons lorsque nous téléphonons. Combien de temps cette information est-elle conservée ? Qui peut y avoir accès ? À quelles fins ?

La "trace" que produit désormais l'usage des techniques appelle la vigilance autant que le faisait jadis le renseignement d'ordre politique ou administratif qui figurait dans un fichier. Car, dans les deux cas, l'enjeu, c'est la liberté. Tant qu'une information personnelle, fût-elle une trace, est conservée, elle peut être utilisée, détournée, portée à la connaissance d'un tiers et accessible à la police, bien des années après. Les fiches d'hôtel ont été supprimées, mais l'autocommutateur téléphonique de l'hôtel permet de savoir qui nous avons appelé. Les écoutes téléphoniques sont étroitement encadrées, mais l'administrateur d'un réseau peut prendre connaissance du contenu de notre messagerie électronique. Les perquisitions policières au domicile des personnes, en principe, ne peuvent pas être opérées de nuit, mais il est possible de reconstituer toute notre navigation, fût-elle de nuit, sur Internet pendant autant de temps que les fournisseurs d'accès conservent nos données de connexion ou le disque dur de notre ordinateur les *cookies* qui y ont été implantés.

Balzac évoquait déjà, dans "Splendeur et misères des courtisanes", "cet océan de renseignements [qui] dort immobile, profond et calme comme la mer. Qu'un accident éclate, que le délit ou le crime se dresse, la justice fait appel à la police et aussitôt, s'il existe un dossier sur les inculpés, le juge en prend connaissance". Il y a près de deux siècles, cet "océan immobile, profond et calme" ne visait que les seuls renseignements de police. Deux siècles plus tard, cet océan est aussi un monde de traces informatiques liées à nos gestes les plus quotidiens.

L'informatisation de nos sociétés et la traçabilité nouvelle que permettent les nouvelles techniques, qu'il s'agisse des moyens nomades (un téléphone portable, une carte à puce, un badge d'accès) ou des réseaux (Internet, intranet d'entreprise) doivent nous inciter plus que jamais à rechercher la juste règle du jeu, le bon équilibre entre informatique et libertés.

Or, cet équilibre ne peut être atteint qu'au travers d'une exigence de retenue. Les possibilités d'intrusion dans la vie privée n'étant, désormais, nullement limitées par la technique qui, bien au contraire, les facilite, et à un degré jusqu'alors jamais atteint, cette exigence doit clairement signifier que les autorités de l'Etat mais aussi les professionnels concernés ne s'autoriseront pas à faire tout ce que permet le développement du "numérique".

Le souci de la personne humaine

Le premier souci du législateur de 1978 a été que la puissance de l'informatique ne conduise pas à l'automaticité de la décision, n'évince pas

l'appréciation individuelle dans le processus de décision. La loi du 6 janvier 1978 a été adoptée à une époque où le casier judiciaire national, notre mémoire des condamnations, venait d'achever son informatisation. Aussi, la préoccupation que l'on ne passe pas d'une justice humaine à une justice automatique rendue non plus par des juges à l'égard de personnes prévenues ou accusées, mais par des machines à l'égard de clones, de portraits-robots, de profils de personnalité, établis à partir de la seule mémorisation des condamnations précédentes, trouve-t-elle un écho dès l'article 2 de la loi : "*aucune décision de justice impliquant une appréciation sur un comportement humain ne peut avoir pour fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé*".

Prudent, le législateur a élargi cette prescription hors le seul domaine judiciaire : "aucune décision administrative ou privée impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé".

La CNIL a eu à apprécier un certain nombre de traitements au regard de cette prescription. L'un des premiers traitements qu'elle eut à examiner, dénommé "GAMIN", avait pour objet de permettre, sur la base des informations de nature médicale et sociale recueillies à partir des certificats de santé établis dans le cadre de la protection maternelle et infantile, la sélection automatique des enfants devant faire l'objet d'une surveillance médico-sociale particulière.

Ce dossier a soulevé dans les années 80-81 de profondes craintes. Sélectionner un enfant sur le fondement de certificats médicaux, de certificats de PMI, n'est-ce pas le ficher à jamais ? Assurer le suivi du nouveau-né, n'est-ce pas le "marquer", d'abord comme étant un enfant qui doit faire l'objet d'un suivi, puis, comme adulte qui a été un enfant suivi ?

Enfin, deuxième préoccupation, non moins essentielle : si le processus de sélection est automatique, comment s'assurer que des enfants qui ne seraient pas sélectionnés par la machine, mais qui auraient également nécessité un suivi médico-social soient repérés ? La Commission, après avoir longuement consulté l'ensemble des acteurs concernés, a rendu en 1983 un avis favorable à ce traitement en y mettant plusieurs conditions et en rappelant qu'en aucun cas le traitement et la sélection telle qu'elle résultait du traitement automatisé, ne devaient constituer le seul fondement du suivi ou de l'absence de suivi de l'enfant.

Dans une recommandation du 13 janvier 1987, la CNIL a d'ailleurs rappelé que "*la présélection par ordinateur des enfants à risques, susceptibles d'une surveillance médicale et sociale particulière, était de nature à porter atteinte à l'identité humaine et à la vie privée et appelait, dans l'esprit de l'article 1er de la loi du 6 janvier 1978, une réserve de principe*". Aussi, la Commission a-t-elle recommandé, d'une part, que les fichiers informatisés de gestion des certificats de

santé des jeunes enfants soient conçus de façon à permettre une séparation entre les données relatives à l'identité des personnes et les renseignements médicaux, et, d'autre part, que les informations nominatives soient effacées dès que l'enfant concerné a atteint l'âge de six ans.

La méthode des profils et les systèmes experts

La méthode des profils utilise la capacité de traitement pour classer les individus au regard de caractéristiques définies a priori ou déterminées après une étude statistique fine, à partir desquelles on va calculer des probabilités. Ces caractéristiques et probabilités figureront dans le logiciel qui pourra ensuite, au regard de critères prédéterminés, classer les personnes, les trier.

Les applications informatiques d'aide à la décision et les systèmes experts font appel à de telles méthodes, fréquentes notamment dans le domaine du recrutement du personnel ou d'estimation d'un risque ("*scoring*") présenté par l'individu en tant que demandeur d'un crédit bancaire, d'une assurance vie ou en tant que contribuable.

C'est ainsi que la Commission a rendu une délibération très importante en 1988 dans le domaine du crédit. La technique du score ou "*crédit-scoring*" repose sur l'attribution automatique d'un certain nombre de "points" aux renseignements qui sont fournis lors de l'examen d'une demande de prêt : traitements et salaires, loyers, autres charges, mais aussi lieu de naissance, surface et situation géographique du domicile, état matrimonial, etc. Selon le total de points recueillis, un crédit sera ou non attribué.

L'intérêt de la Commission s'est manifesté dans cette matière à la suite de la déclaration d'un traitement de "*crédit-scoring*" qui attribuait un tel nombre de points aux Français nés dans un département ou Territoire d'Outre-Mer qu'il leur devenait, en pratique, impossible de se voir consentir un prêt, quelle que soit, par ailleurs, leur situation financière.

La CNIL a alors indiqué, d'une part, que le calcul automatique du risque constituait un traitement automatisé d'informations nominatives qui devait, à ce titre, être déclaré à la Commission, d'autre part et surtout, que les caractéristiques du processus d'établissement du score devaient lui être communiquées afin qu'elle puisse s'assurer que les méthodes mises en oeuvre ne conduisent pas inéluctablement à des décisions de rejet qui reposeraient sur des critères discriminants illégitimes, voire illégaux.

Il s'agissait pour la CNIL de s'inspirer des dispositions de l'article 3 de la loi qui constituent, d'une certaine manière, la sanction qui s'attache à l'interdiction posée par l'article 2. Cet article dispose que "*toute personne a le droit de connaître*

et de contester les informations et les raisonnements utilisés dans les traitements automatisés dont les résultats lui sont opposés". Depuis lors, les établissements qui recourent à la technique du score doivent faire connaître à la CNIL les critères qui sont utilisés et leur pondération.

Dans le même esprit, par une délibération du 22 décembre 1998, qui fait à ce jour l'objet d'un recours devant le Conseil d'Etat, la Commission a estimé que l'utilisation de la nationalité comme variable du "score", pondérée différemment selon la nationalité du demandeur au crédit, n'était pas "pertinente" au sens de l'exigence posée par l'article 25 de la loi du 6 janvier 1978.

Les systèmes d'information géographique

Les systèmes d'information géographique consistent, à partir du recoupement d'informations, à caractériser non pas le "profil" d'une personne, mais celui d'un territoire (l'îlot) dont les caractéristiques seront supposées être celles du groupe, considéré comme homogène. L'îlot, unité statistique de base, correspond à un "pâté de maisons" ou à une zone de peuplement considérée comme homogène et comportant en moyenne 150 habitants.

L'îlotypage est utilisé de manière courante à des fins de prospection commerciale. Il s'agit alors, par le maillage du territoire, de limiter la prospection commerciale aux seules zones géographiques ou quartiers supposés correspondre à la "cible commerciale" du produit. De telles pratiques, au demeurant courantes, n'appellent aucune observation particulière. Il n'en est pas de même lorsque "l'ilôtypage" est dit "négatif". Tel est le cas quand il s'agit, non plus de sélectionner une cible commerciale, mais d'exclure toutes les personnes d'un même îlot considéré comme étant "à risque".

Rapporté au crédit, il s'agirait alors d'exclure du crédit ou de procéder systématiquement à des vérifications complémentaires en fonction de l'adresse (quartier, immeuble) du demandeur au crédit.

La CNIL a ainsi été saisie, en mars 2000, d'une déclaration déposée par un établissement de crédit qui évoquait une utilisation future de l'îlotypage lors de l'examen préalable des demandes de crédit. Cette technique devait permettre de déterminer la cohérence d'un dossier au regard des caractéristiques présentées par la population du pâté de maison (îlot) qu'habite le demandeur, par exemple par comparaison entre le revenu déclaré et le revenu moyen de l'îlot.

De tels procédés sont très largement utilisés aux Etats-Unis et en Grande-Bretagne et un établissement de crédit d'origine anglo-saxonne, en cours d'implantation en France, a souhaité recueillir l'opinion de la CNIL sur ce point. La Commission s'est évidemment montrée très réservée à l'égard de cette

nouvelle géographie dessinant des profils de groupes pouvant conduire à la prise de décisions automatiques, sans considération pour les personnes. Les risques de dérives et de discriminations que de telles pratiques sont susceptibles de générer appellent incontestablement à une réponse très ferme.

C'est la raison pour laquelle, d'ailleurs, la CNIL, en liaison avec l'INSEE et dès le recensement général de la population de 1990, a établi des règles de cession de résultats statistiques à un niveau géographique d'un certain seuil, de sorte, d'une part, d'éviter tout risque de réidentification des personnes par recoupement de fichiers et, d'autre part, le risque qu'une "typologie" trop fine ou trop précise de profils de population conduise inéluctablement à la prise de décision sur le seul fondement d'une adresse.

Le "droit à l'oubli"

Le "droit à l'oubli" a souvent été présenté comme la principale garantie face à la mémoire de l'ordinateur.

Jusqu'à l'informatisation de nos sociétés, l'oubli était une contrainte de la mémoire humaine, certains diraient une fatalité. Avec l'informatisation, la capacité de mémorisation des ordinateurs de plus en plus puissante, les possibilités de consultation les plus souples et les plus précises, l'oubli relève désormais de la seule volonté humaine.

Le "droit à l'oubli" n'est pas nouveau ; il n'est pas né avec la loi du 6 janvier 1978 qui d'ailleurs ne le consacre pas même s'il inspire toute notre législation. Ce droit est sans doute né avec l'idée même d'équilibre. Le code pénal le prévoit en plusieurs de ses dispositions: l'amnistie efface l'infraction; la grâce relève de la condamnation; la réhabilitation est une manière d'oubli collectif lorsque le condamné n'a pas récidivé; certaines condamnations peuvent être automatiquement effacées après un temps d'épreuve; l'action publique contre les auteurs d'infractions se prescrit: on n'a plus le droit de rechercher un criminel passé un délai de dix ans; la condamnation elle-même se prescrit: on ne peut plus faire exécuter une condamnation correctionnelle plus de cinq ans après son prononcé.

Quelques illustrations

Ce droit à l'oubli se traduit dans nos législations de protection des données informatisées de diverses manières.

La première de ces manifestations porte sur la durée de conservation des informations qui doit être limitée et justifiée par la finalité du traitement.

La convention 108 du Conseil de l'Europe, qui est directement applicable dans notre ordre interne depuis 1985, est sur ce point sans ambiguïté. Son article 5 dispose que "*les données à caractère personnel faisant l'objet d'un traitement automatisé sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées*".

Les exemples abondent d'interventions de la CNIL à ce sujet, tant les tentations sont fortes. C'est ainsi que la Commission a recommandé que les autocommutateurs mis en place sur les lieux de travail ou dans les lieux de séjour (hôpitaux, maisons de retraite, etc.), qui permettent d'identifier toutes les lignes appelées depuis tel poste téléphonique, ne conservent pas trace des numéros appelés, poste par poste, après deux périodes de facturation, ou après le règlement de la facture.

Dans un autre domaine, celui de l'assurance-vie, la Commission, après avoir accompli plusieurs missions de vérifications des fichiers dits de "risques aggravés", qui recensent les personnes ayant fait l'objet d'un refus total ou partiel d'assurance ou qui sont soumises à une surprime en raison d'une pathologie déterminée, a recommandé que soient effacées de tout support informatique, les informations de nature médicale dès lors que la demande de souscription a été refusée. Pas de lien contractuel à l'issue des examens médicaux ; pas de conservation sur informatique des informations médicales recueillies.

Le droit d'être radié d'un fichier après un certain délai ou ce que nous appelons le droit d'opposition pour raisons légitimes sont également d'autres modalités d'un droit à l'oubli. Aucune trace d'impayé ne peut être conservée dans un fichier central ou interprofessionnel aussitôt la dette réglée.

Une nécessaire conciliation entre "droit à l'oubli" et les nécessités de la recherche scientifique

Evidemment, ce "droit à l'oubli" doit être concilié avec les nécessités de la recherche scientifique. Tel est d'ailleurs l'un des apports substantiels de la directive européenne du 24 octobre 1995 qui aménage plusieurs dérogations aux règles ordinaires de la protection des données personnelles au bénéfice de la "recherche scientifique, statistique et historique". Ainsi, l'exploitation des données personnelles et leur conservation à de telles fins apparaissent-elles consacrées comme constituant des finalités légitimes et pour tout dire "naturelles" de tout traitement automatisé d'informations nominatives. Sur ce

point, la France n'a pas tardé puisque la loi du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec l'administration a consacré ce principe.

Il s'agit dès lors, non pas d'opposer la protection des données personnelles à la recherche scientifique ou au "devoir de mémoire" mais bien de concilier l'une et l'autre.

Ainsi, la recherche historique ne saurait justifier que des données recueillies par la police judiciaire soient conservées dans les commissariats plus longtemps que le justifie la finalité d'ordre public qui préside à leur collecte. Ces données pourront être conservées si elles revêtent un intérêt historique, mais nullement par la police et exclusivement par les services des archives de France dans les conditions qui assurent pleinement le respect de cette finalité historique.

Dans le même esprit, l'évaluation statistique de certaines politiques publiques commande de pouvoir conserver des données sur de longues périodes. Mais l'exploitation de telles données, à de telles fins, ne doit pas conduire à multiplier les "casiers sociaux" ou les "casiers médicaux" qui seraient de nature à susciter des risques importants de discrimination à l'égard des personnes concernées. En ce domaine plus qu'en d'autres, les outils techniques peuvent permettre de réaliser le juste arbitrage entre des intérêts contradictoires. Ainsi, en matière d'informations statistiques sur l'activité et le coût des soins dans les établissements de santé, des logiciels dits "d'anonymisation" permettent de transformer de manière irréversible des données nominatives en un numéro non signifiant qui permettra d'associer, sur de longues périodes, les données relatives à un même individu sans qu'il soit possible de l'identifier. L'utilisation de tels logiciels d'anonymisation a été préconisée par la CNIL notamment en matière de recherches statistiques sur les bénéficiaires du RMI et lors de la mise en place du fichier épidémiologique de séropositivité. Ainsi, la recherche peut-elle disposer de nombreuses données sans qu'à aucun moment les personnes ne soient fichées sous leur identité. L'outil technique aura permis le développement des "sujets de recherche" en préservant "la" personne.

Il reste que toutes les traces de nos activités les plus intimes, et tout particulièrement celles qui sont produites par la technique, ne sauraient être conservées à jamais au seul motif qu'elles existent.

Droit à l'oubli et traces informatiques

Le développement des nouvelles applications informatiques — notamment l'usage désormais courant des cartes à puce dites "multiservices" — ne rendent pas obsolètes de tels principes. Bien au contraire, la commodité d'usage de tels instruments peut parfois faire oublier que chacune de leur utilisation est consignée dans une mémoire infaillible.

Ainsi, la Commission a été saisie d'un projet consistant à doter les usagers de services de transports d'une grande ville d'une carte à puce nominative, achetée et chargée depuis un point de vente. Pouvant être utilisée dans le métro, le bus, les parkings privés, le passage d'un tunnel, la carte devait permettre de régler à distance le prix de ces services, l'ensemble des informations nominatives étant conservé en mémoire dans un ordinateur central afin de pouvoir débiter le coût des transactions.

La Commission a donné un avis favorable à un tel projet après qu'il eut été convenu que les informations nominatives sur l'utilisation de la carte ne seraient pas conservées au-delà d'une semaine, et surtout que les habitants de la ville pourraient continuer à bénéficier des services publics de transport de manière anonyme, s'ils le souhaitaient.

Autre exemple : la CNIL a été saisie par une société concessionnaire d'une autoroute d'un projet informatique consistant, grâce à des capteurs placés de part et d'autre des postes de péages, à enregistrer le numéro minéralogique de tous les véhicules afin, notamment, de calculer les temps de passage aux péages, d'apprécier les flux de trafic, de repérer en temps réel les anomalies, les informations - en l'espèce, le numéro minéralogique de chaque véhicule - devant être conservées pendant un mois.

La Commission a estimé, compte-tenu notamment de cette durée de conservation, qu'un tel projet ne pourrait recueillir, en l'état, un avis favorable dans la mesure où il avait pour effet d'identifier - au moins indirectement - tous les véhicules empruntant cette autoroute, mettant un terme à l'anonymat de nos déplacements et entamant ainsi la liberté de circulation.

Enfin, Internet soulève une question de même nature. Les traces de nos connexions sont conservées par les intermédiaires techniques de l'Internet que sont les hébergeurs et les fournisseurs d'accès. Les "fichiers logs" conservent l'enregistrement des données de connexion: l'adresse de la machine qui s'est connectée, que les spécialistes appellent "adresse IP" qui constitue la plaque minéralogique de chaque ordinateur, toutes les requêtes que l'ordinateur connecté aura lancées, les services utilisés (messagerie électronique - web) ainsi que l'heure exacte de la connexion.

Ces informations de nature technique peuvent évidemment être rapprochées — grâce à l'adresse de l'ordinateur — de l'identité et de l'adresse physique de l'internaute connues du fournisseur d'accès dont il est le client. Ces informations devraient normalement être volatiles, elles ne le sont pas et sont conservées à des fins commerciales, mais aussi à des fins de sécurité publique sur le réseau. Pendant combien de temps, de telles traces sur nos activités les plus personnelles doivent être conservées ?

Cette question est essentielle, non seulement au regard des règles qui président à la protection des données personnelles, mais, plus généralement, au

regard du principe de proportionnalité qui résulte de l'article 8 de la Convention Européenne des Droits de l'Homme.

VERS LA RECONNAISSANCE DE LA PROTECTION DES DONNÉES PERSONNELLES COMME UNE GARANTIE FONDAMENTALE DES LIBERTÉS

Ces observations expliquent sans doute que le principe d'une protection (improprement dite "des données personnelles" alors qu'il s'agit d'une protection des personnes à l'égard du traitement automatique des données qui les concernent) soit, dans bien des Etats, consacré au niveau constitutionnel, plus encore lorsque ces Etats ont connu des régimes autoritaires.

On sait, depuis la décision 92-316 du 20 janvier 1993, que le Conseil Constitutionnel rattache la législation relative à l'informatique, aux fichiers et aux libertés aux "dispositions protectrices de la libertés individuelle", elle-même à valeur constitutionnelle et que, dans sa décision 98-405 du 29 décembre 1998, le Conseil Constitutionnel a invoqué les "exigences constitutionnelles relatives à la protection de la vie privée et de la liberté individuelle".

L'Union européenne elle-même a souhaité faire figurer la protection des données personnelles au titre des droits fondamentaux proclamés par la Charte dont elle s'est dotée au sommet de Nice.

L'exigence posée par l'article 7 de cette Charte qu'une autorité de contrôle indépendante soit instituée manifeste, sans aucun doute, le rôle qui est encore attendu de telles autorités à l'heure du "tout numérique".

"L'organe de la conscience sociale" écrivait, il y a plus de 20 ans, Bernard Tricot en appelant de ses vœux la création d'une autorité ad hoc. Cette exigence demeure, plus que jamais, d'actualité.