INTRODUCTION

La cause est entendue : le monde s'est converti au numérique. Et cette conversion est révolutionnaire. Dans tous les domaines de l'activité humaine, des techniques futuristes (au nom se terminant souvent par le suffixe *-tique* : informatique, robotique, domotique…) appréhendent le réel comme de l'*information* qui, codée sous forme binaire et structurée en *données*, peut être *traitée* par des *systèmes* d'une puissance inouïe. Ces nouvelles technologies de l'information et de la communication, les NTIC, organisent désormais notre vie et façonnent nos comportements. Elles concernent toutes nos activités professionnelles ou familiales, individuelles ou ludiques dans tous les secteurs : la banque, l'industrie, le commerce, les jeux, les médias, les télécommunications, les loisirs, mais aussi la défense, l'espace, l'art, l'économie, l'enseignement, les transports ou le droit… Un quart de la croissance mondiale est déjà généré par les NTIC qui ont représenté 2 750 milliards d'euros dans le monde en 2007. L'Informatique est partout. Elle gère des fichiers, constitue des bases de données. Elle régule la circulation dans les grandes villes. Elle surveille les barrages hydrauliques. Embarquée, elle conduit les trains ou pilote les avions.

Mais c'est Internet qui a donné à la révolution numérique son aspect le plus spectaculaire. Tandis que chacun est désormais rompu au courrier électronique, on vit de plus en plus souvent en ligne. C'est sur eBay qu'on achète un livre (ou un meuble), par Google qu'on cherche un renseignement, sur Legifrance qu'on consulte la loi. L'administration devient électronique et les dossiers se dématérialisent. Grâce à la Toile, on blogue, on « chate », on débat dans les forums. On échange de la musique. On parie. On va au cinéma. Et, depuis le web 2.0, on peut avoir une vie sociale en ligne grâce aux réseaux du même nom. Bientôt même, tout le monde votera en ligne. Et le net de demain est déjà là : « mobile net », accessible depuis les portables dont 3 milliards sont en circulation dans le monde. Les Français sont conquis par cette nouvelle manière de vivre : 95 % des foyers étaient raccordés au milieu de l'année 2008. Quant aux pouvoirs publics, ils sont résolument favorables. En 2003, Internet était déclaré d'utilité « tout public ». Depuis 2004, la France a une loi pour la confiance dans l'économie numérique. Et depuis 2008, il existe

un secrétariat au développement de l'économie numérique, l'un des premiers en Europe. Le président rêve d'une république numérique. Tout serait donc pour le mieux dans le meilleur des mondes numériques...

Pourtant tout n'est pas si rose. L'univers virtuel est rempli de dangers. Les fichiers qui se remplissent de nos données personnelles se multiplient et s'interconnectent. Alors que la menace qu'ils constituent pour les libertés s'aggrave, les instances chargées de leur contrôle manquent chaque jour un peu plus de pouvoirs et de moyens. La géolocalisation, la biométrie, le *profiling* et le *scoring* permettent de redoutables atteintes à la vie privée que les nanotechnologies rendent plus pernicieuses encore. Plus que jamais, la collecte frauduleuse de données est un risque majeur. Sur le net, des escrocs d'un nouveau type, les *phishers*, construisent des sites factices pour nous extorquer les identifiants avec lesquels ils vident nos comptes en banque. Le réseau est devenu un espace de perdition. La contrefaçon y prospère plus que partout ailleurs, favorisée par l'extrême reproductibilité du support numérique. Piller la propriété intellectuelle de millions d'auteurs est devenu une activité de masse dont on revendique la licéité au péril de l'industrie du disque si bien que le législateur doit revoir la protection du droit d'auteur. Dans le même temps, la Toile se révèle propice à une stupéfiante prolifération de la pédopornographie. Un commerce planétaire d'images de pornographie infantile est né dont les adeptes sont constitués en organisations de dimension internationale. Les opérations de police, d'une ampleur jamais vue, doivent être menées sur plusieurs continents à la fois. La loi doit créer de nouvelles incriminations et autoriser les enquêteurs à pratiquer l'infiltration électronique.

Pour autant, la figure historique du *hacker*, bidouilleur génial, n'en devient pas plus sympathique. Les casseurs de logiciel ont, eux aussi, suivi la tendance. Finis les défis spectaculaires aux enjeux symboliques. Les pirates d'aujourd'hui sont des professionnels discrets que l'argent seul intéresse. Aux coups d'éclat individuels ont succédé des actions organisées suivant des méthodes maffieuses. Abrités derrière d'éphémères adresses IP, des gangs sans visage manœuvrent des armées de robots avec lesquelles ils bombardent, rackettent et détroussent. Un incroyable marché noir du crime numérique se développe sur la Toile. Chacun peut y acheter le dernier cri des logiciels malfaisants ou louer une armée de mercenaires informatiques. Le droit pénal français permet bien, depuis 1988, de poursuivre les atteintes aux systèmes de traitement automatisé de données. Mais les cas jugés ne se comptent que par dizaines : les malfaiteurs opèrent, le plus souvent depuis l'étranger.

Au moins le net reste-t-il un incomparable moyen d'expression. Le sentiment d'extrême liberté qu'il donne est toutefois trompeur. Injures, diffamations et autres délits de presse y sont réprimés. Et les blogueurs, organisateurs de forums ou autres hébergeurs y répondent – avec étonnement trop souvent – de tous les contenus illicites dont ils ont permis la publication. C'est le prix pour éviter une censure d'autant plus tentante pour les pouvoirs publics qu'elle est techniquement facile par filtrage. Il fallait, en tous les cas, enrayer l'engouement suscité par le web pour la violence filmée en direct. Depuis 2007, la loi pour la prévention de la délinquance punit ceux qui enregistrent des violences comme les auteurs de ces violences. Cela suffira-t-il à éradiquer le *happy slapping* ? Rien n'est moins sûr. Internet est le réseau de tous les possibles. N'est-il pas aussi le lieu d'émergence d'un cyberterrorisme ?

De violentes attaques électroniques d'origine incertaine ont, en 2007, paralysé tout un pays pendant plusieurs jours. Alors que la Toile est devenue le sanctuaire d'Al-Quaeda, une vigilance absolue s'impose. S'inspirant des Britanniques qui ont élucidé les sanglants attentats de 2005 à Londres grâce à la vidéosurveillance, la France, depuis la loi antiterroriste de 2006, couvre ses rues de caméras pour filmer les trottoirs. Elle a aussi mis le net sous surveillance. Comme tous les intermédiaires techniques, les cybercafés sont désormais tenus de conserver les données de connexions de leurs clients pour les remettre à la police au seul soupçon de celle-ci, sans contrôle d'un juge. Le dispositif antiterroriste français est assurément efficace. Mais à quel prix ? Selon The Privacy International, la France a rejoint, en 2007, les pays dont les populations sont considérées comme les plus surveillées au monde.

Ainsi les nouvelles technologies dessinent-elles une société de l'information qui suscite autant d'attrait que de méfiance. C'est le sujet de ce livre. Sept chapitres et des annexes le composent.

1. Le premier chapitre est consacré aux difficiles rapports entre Informatique et libertés.

2. Le deuxième est dédié au pillage de la propriété intellectuelle sur Internet.

3. Le troisième présente le triste bilan des escroqueries numériques (*scam* et *phishing*).

4. Le quatrième traite de l'indispensable protection des mineurs face à la pornographie et la pédopornographie en ligne.

5. Le cinquième dessine les limites de la liberté d'expression dans l'univers numérique.

6. Le sixième montre que le *hacking* est toujours vivant sous une forme autrement plus inquiétante qu'à ses origines.

7. Le dernier cherche à faire le point sur le cyberterrorisme.

À chaque chapitre correspond, en annexe, une anthologie des textes réprimant la cybercriminalité décrite. Les éléments d'une bibliographie sont fournis. Les acronymes de l'univers digital sont énumérés avec leur sens. Enfin, deux index, l'un thématique, l'autre des noms propres donnent au lecteur la possibilité de consulter l'ouvrage suivant plusieurs clés.

Chapitre 1

Souriez, vous êtes fiché !

De tout temps la mise en fiches d'une population a constitué une menace pour les libertés individuelles. Sans remonter jusqu'aux pharaons dont les scribes ont permis d'asservir les Égyptiens, il faut se souvenir de l'usage sinistre du « fichier juif » par Vichy durant l'Occupation. L'avènement de l'informatique en France dans les années soixante et, avec elle, des fichiers numériques, portait en germe un danger considérable. L'extraordinaire efficacité de cette technologie n'allait-elle pas faciliter la mise en fiches de tous les Français et permettre de suivre à la trace les moindres faits et gestes de chacun, tout en fournissant d'innombrables informations sur les caractéristiques personnelles les plus intimes : religion, origine ethnique, orientation sexuelle, opinions politiques... ?

1.1 Safari

Le danger s'est montré au grand jour en 1974. Sous la plume de l'un de ses chroniqueurs fameux, Philippe Boucher, le journal *Le Monde* révélait l'existence du projet Safari alors que le ministre de l'Intérieur de l'époque s'appelait Jacques Chirac[1]. Il s'agissait de connecter entre eux 400 fichiers nationaux en permettant ainsi le traitement de toutes les données contenues dans cent millions de fiches. La révélation de ce projet provoqua un scandale. Le gouvernement recula. Le parlement fut saisi. Et c'est ainsi que quatre ans plus tard, le 6 janvier 1978, fut votée la loi relative à l'informatique, aux fichiers et aux libertés dont l'article premier proclame, comme en écho à l'émotion qu'avait soulevée le projet Safari : « L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle 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. »

Démocratisation

De tous les nombreux remaniements de la « LIL », le plus important fut celui de 2004[2]. La loi avait vieilli. Les fichiers porteurs de données personnelles des individus n'étaient plus entre les seules mains des pouvoirs publics. L'informatique s'était démocratisée : les fichiers étaient partout. Il fallait en tenir compte. Ce fut, dans une certaine mesure, au bénéfice des fichiers

1. « Safari, ou la chasse aux Français » titrait *Le Monde* du 21 mars 1974.
2. Par la « loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ».

étatiques, pourtant les plus étoffés. Ils échappèrent au contrôle direct de la Commission nationale de l'informatique et des libertés (la CNIL) instituée par la loi du 6 janvier 1978. Ainsi le STIC (système de traitement informatique des infractions constatées). La CNIL avait bataillé pour obtenir la rectification des très nombreuses erreurs qu'elle avait constatées[1] sur ce fichier qui n'avait pendant longtemps eu aucune existence légale. En vain. Il devenait après 2004 l'un des fichiers « de souveraineté » qui n'étaient plus de sa compétence. Il reste que la réforme de 2004 ayant – enfin – transcrit en droit interne une directive européenne de 1995, la France dispose aujourd'hui d'un système juridique relativement élaboré de protection des libertés face aux risques que constituent les fichiers de données personnelles. Quel est ce régime ?

Donnée personnelle, fichier, traitement

La loi de 1978, telle que modifiée en 2004, commence par des définitions et elle prend soin de définir en premier une notion qui est la clé de voûte de tout le système : celle de *donnée personnelle*. Qu'est ce qu'une donnée personnelle ? C'est l'un de ces renseignements dont les fichiers fourmillent – un nom, un numéro, une adresse… – ayant la particularité de permettre soit directement, soit indirectement l'identification d'une personne. Prenez un prénom. Tout seul, il ne suffit pas à constituer une identité. Mais rapprochez-le d'un numéro de téléphone et vous aurez le nom de famille, donc l'identité de quelqu'un. Voilà ce que la loi appelait, avant 2004, une *information nominative*. Mais l'expression est, à juste titre, apparue trop restrictive dans la mesure où il n'est pas nécessaire qu'un nom apparaisse pour qu'une identification soit possible. Une donnée personnelle, ce peut être bien sûr, un nom, un prénom, ou une date de naissance. Mais ce peut être aussi une adresse électronique, l'adresse IP d'un ordinateur, un numéro de téléphone ou le numéro d'immatriculation d'un véhicule. Ce peut être encore le numéro d'une carte de paiement, une empreinte digitale ou une photographie…

Si les données personnelles sont au cœur du dispositif légal, c'est parce que ce sont de véritables parcelles de vie privée que, tous les jours, en effectuant des actes banals de la vie quotidienne, nous laissons aux mains des autres. Avons-nous un entretien d'embauche ? Les notes prises par notre interviewer, ce sont des données personnelles que nous lui laissons. Les éléments de solvabilité que nous a demandés notre banquier ? c'en sont d'autres. Et quand nous payons par carte bancaire au péage de l'autoroute, nous indiquons notre

1. 25 % de rectifications sur les éléments vérifiés en 2001, 37 % 2002 et 22 % en 2003.

numéro de carte, donc notre nom, le lieu ou nous nous trouvons, l'heure qu'il est, la distance que nous avons parcourue... Savons-nous, même, dans ce cas, à qui nous confions tout cela ?

Toute opération

Certes, le plus souvent, une donnée personnelle ne confère pas, à celui qui la détient le pouvoir de menacer notre vie privée ni notre liberté Mais il en va différemment quand cette donnée peut faire l'objet de rapprochements avec d'autres. Voilà pourquoi, après avoir défini la donnée personnelle, la loi du 6 janvier 1978, définit ce qui – en bien ou en mal – en permet l'exploitation : le *fichier*. C'est, dit la loi, un ensemble stable et structuré de données pouvant recevoir un *traitement*. Et le traitement, c'est toute opération sur le fichier, depuis la collecte jusqu'au verrouillage ou à l'effacement en passant par l'enregistrement, l'organisation, la conservation, l'extraction, le rapprochement ou l'interconnexion. Autrement dit, le fichier c'est la collection de données au repos. Le traitement c'est l'action de faire parler le fichier. La loi s'applique donc aux fichiers comme aux traitements. Que prévoit-elle ?

Fichiers sensibles et fichiers de souveraineté

Ainsi défini, un fichier de données personnelles ne peut exister qu'à certaines conditions. Tout dépend de la catégorie à laquelle il appartient. Depuis 2004, on ne distingue plus entre fichier public et fichier privé. La question est désormais de savoir si un fichier contient ou non des *données sensibles*. Sont sensibles au regard de la loi les données qui ont trait à l'origine raciale ou ethnique des personnes, à leurs opinions politiques ou religieuses, à leur appartenance syndicale, ou encore à leur santé ou leur vie sexuelle. La collecte de telles données étant, en principe, interdite, les fichiers n'en contenant pas sont l'immense majorité. Leur création n'est soumise qu'à une *déclaration préalable* auprès de la CNIL. Le déclarant devra toutefois certifier la conformité de son traitement à l'une des normes régulièrement élaborées par la CNIL. En pratique la CNIL dispense de déclaration certains fichiers privés conformes à un type dont elle a pu vérifier qu'il ne présentait pas de danger. Ainsi a-t-elle, en novembre 2005, dispensé les *blogs,* tout en rappelant à leurs responsables qu'ils doivent obtenir l'accord de tous ceux dont ils collectent des données personnelles. Sont également dispensées de déclaration les personnes morales qui se sont adjoint un *correspondant informatique et libertés,* courroie de transmission entre la CNIL et ses « administrés » instituée par la loi de 2004.

Autorisation préalable

La création des fichiers sensibles devra, en revanche, avoir reçu une *autorisation préalable* de la CNIL. Celle-ci peut ainsi s'assurer qu'ils ne constituent pas une menace pour les libertés de ceux qui y sont fichés. Le cas échéant, la CNIL peut même conditionner l'octroi de son autorisation à certaines mesures de sécurité. Une des innovations – très critiquée – de la révision de la loi, en 2004, concerne les grands fichiers de l'État en matière de sécurité ou de défense. La création de ces *fichiers de souveraineté* échappe désormais à la CNIL même quand ils contiennent des données personnelles sensibles, ce qui est souvent le cas. Leur création intervient par décret en Conseil d'État, la CNIL étant seulement consultée. Si la raison d'État le commande, la création de tels fichiers peut même rester secrète.

1.2 Les sept commandements

En tout état de cause, les utilisateurs de traitements ou de fichiers doivent respecter les obligations que la loi leur impose. Ces obligations sont au nombre de sept et concernent la collecte, la finalité, la conservation, la sécurité, la confidentialité, l'information et la déclaration.

1. *La collecte des données doit être loyale*. Cela signifie d'abord qu'il faut, en principe, recueillir le consentement d'une personne pour utiliser une information qui l'identifie. Cela signifie, ensuite, que les données traitées doivent être exactes, complètes et mises à jour. Cela veut dire, enfin, que, sauf dérogation, il n'est pas possible de collecter des données sensibles. La violation de cette obligation est une faute pénale. En effet collecter des données personnelles par un moyen frauduleux, déloyal ou illicite est un délit prévu par l'article 226-18 du code pénal qui le réprime de 5 années d'emprisonnement et 300 000 euros d'amende.

2. L*a finalité des traitements doit être respectée.* Qu'est-ce à dire ? Que tout fichier doit avoir un objectif précis et que les informations exploitées doivent être cohérentes par rapport à cet objectif. Elles ne peuvent être réutilisées pour une autre finalité. Sinon c'est un détournement de finalité que l'article 226-21 du code pénal considère comme un délit passible de 5 années d'emprisonnement et 300 000 euros d'amende.

3. *La durée de conservation des données doit être respectée.* Cette durée, qui dépend de la nature des données et de la finalité du fichier, fait partie

de la déclaration (ou de l'autorisation). Aux termes de l'article 226-20 du code pénal, la conservation des données pour une durée supérieure à celle qui a été déclarée est un délit passible de 5 années d'emprisonnement et de 300 000 euros d'amende.

4. *La sécurité des données doit être assurée*. Il faut protéger les fichiers. Ce qui veut dire assurer la protection physique des locaux et celle, logique, du système d'information. Le non-respect de l'obligation de sécurité est un délit prévu par l'article 226-17 du code pénal qui le punit par 5 années d'emprisonnement et 300 000 euros d'amende.

5. *La confidentialité des données doit être respectée*. Seules des personnes autorisées peuvent accéder aux données contenues dans un fichier. Il peut s'agir de personnes explicitement désignées pour en obtenir régulièrement communication ou de *tiers autorisés* pour les recevoir de façon ponctuelle ou motivée (police, fisc). La communication d'informations à d'autres gens est interdite. La communication d'informations à des personnes non autorisées est un délit prévu par l'article 226-22 du code pénal. La peine encourue est de 5 ans d'emprisonnement et de 300 000 euros d'amende. Si, la divulgation a été commise par imprudence ou négligence, la peine est de 3 ans d'emprisonnement et 100 000 euros d'amende.

6. *L'information des personnes concernées doit être faite*. Les personnes concernées par un fichier ont des droits. Le responsable du fichier doit leur permettre de les exercer. Pour cela il doit leur communiquer son identité, la finalité de son traitement, le caractère obligatoire ou non des réponses, l'existence de droits ainsi que les transmissions envisagées du fichier. Le refus ou l'entrave au bon exercice des droits des personnes est une contravention prévue par le décret 81-1142 qui est punie, conformément à l'article 131-13 du code pénal, de 1500 euros par infraction constatée et de 3000 euros en cas de récidive.

7. Enfin, on le sait, *il faut déclarer le fichier*. Déclarer ou soumettre à autorisation quand c'est nécessaire. Le non-accomplissement des formalités déclaratives est un délit, prévu par l'article 226-16 du code pénal. Il est passible de 5 années d'emprisonnement et de 300 000 euros d'amende.

Les droits du fiché

Si les responsables de fichiers ont des obligations, c'est bien pour permettre le respect des droits des personnes fichées. La loi les appelle *personnes concernées*. Quels sont leurs droits ?

1. Le premier droit, qui commande tous les autres, est *le droit à l'information.* Quiconque est fiché a le droit, non seulement de le savoir, mais de savoir où et comment. En vérité, ce droit du fiché dépend du respect par le ficheur de son obligation de collecte loyale. C'est en mettant en œuvre son fichier ou traitement de données personnelles que le responsable devra fournir à la personne fichée les informations prévues par la loi, respectant par là le commandement n° 6. Le droit à l'information a toutefois des limites. Il est allégé lorsque les données collectées sont anonymisées ou qu'elles ne sont pas recueillies auprès de la personne concernée. Il est exclu pour les fichiers de police, de gendarmerie ou relatifs à des condamnations pénales (dans ces fichiers-là on peut être fiché sans le savoir).

2. Le deuxième droit du fiché est *le droit d'accès*. C'est un véritable droit d'entrée dans le fichier. Toute personne peut, en vertu de ce droit, interroger le responsable d'un fichier ou d'un traitement pour savoir s'il détient des informations sur elle. Si c'est le cas elle peut en obtenir copie et se faire expliquer le procédé informatique qui a contribué à produire une décision la concernant (scoring, segmentation, profil etc.). Elle peut même faire rectifier ou effacer les données la concernant. Le droit d'accès ne doit toutefois pas être exercé de manière abusive. Si c'était le cas, le responsable du fichier pourrait refuser de donner suite à la demande d'accès.

   Lorsque la demande concerne un fichier de police ou de gendarmerie ou un traitement visant à rechercher, prévenir ou contrôler les infractions ou à recouvrer des impositions, c'est le régime particulier du *droit d'accès indirect* qui s'applique. Le droit s'exerce alors par l'intermédiaire d'un commissaire de la CNIL. Celui-ci effectue les investigations utiles. Il fait procéder aux modifications nécessaires comme par exemple la rectification ou l'effacement de données inexactes. La CNIL notifie ensuite au demandeur qu'il a été procédé aux vérifications nécessaires et elle lui indique les voies de recours.

3. *Le droit de rectification* est un complément du droit d'accès. Il concerne le cas où ont été décelées des inexactitudes ou des données interdites concernant une personne. Celle-ci peut alors faire rectifier, compléter,

actualiser, verrouiller ou effacer les données. À ce titre, par exemple, les héritiers d'une personne décédée peuvent exiger que le responsable d'un traitement comportant des données concernant le défunt prenne en considération le décès et procède aux mises à jour nécessaires.

4. *Le droit d'opposition* est le plus fondamental. Il permet à quiconque de refuser, pour des motifs légitimes de figurer dans un fichier. Toute personne peut même sans motif légitime, refuser que les données qui la concernent soient utilisées à des fins de prospection, en particulier commerciales. L'exercice de ce droit se manifestera, par exemple, par le refus de répondre à une collecte non obligatoire de données ou par le refus de donner l'accord obligatoire pour une collecte de données sensibles. Ce pourra aussi être par une demande de radiation des données contenues dans des fichiers commerciaux. Cependant le droit d'opposition n'existe pas pour de nombreux fichiers du secteur public comme ceux des services fiscaux, des services de police, des services de la justice ou de la sécurité sociale.

1.3 Collectes interdites

Entre les utilisateurs de fichiers qui ont des obligations à respecter et les personnes fichées qui ont des droits à faire valoir, la CNIL joue évidemment un rôle essentiel. Le nombre des déclarations de fichiers qu'elle reçoit suffirait à le montrer. En 2005 elle a enregistré 80 677 nouveaux traitements, ce qui portait le nombre des fichiers qui lui ont été déclarés depuis 1978 à 1 088 593. Dans le cadre de cette compétence, la CNIL est amenée à prendre position lorsqu'elle dit « non » à certains traitements. C'est l'occasion pour elle de préciser sa doctrine et d'être le baromètre de l'atmosphère numérique en faisant connaître l'état des menaces. Les exemples qui suivent concernent des personnes privées. Ils montrent que l'imagination est facilement stimulée par les avancées technologiques. Et que la menace des fichiers informatiques sur les libertés n'a rien de théorique.

Biométrie

Le 12 janvier 2006 la CNIL a refusé d'autoriser quatre *dispositifs biométriques,* c'est-à-dire des procédés utilisant le corps humain comme moyen

d'identification. Il s'agissait de traitements destinés à contrôler l'accès[1] à certains lieux ainsi que la gestion des horaires. Dans l'examen des dispositifs biométriques, la CNIL prend en considération le type de biométrie utilisée. Elle distingue la biométrie « à trace » et la biométrie « sans trace » selon qu'il est possible ou non de récupérer une donnée biométrique à l'insu de la personne. Il s'agissait de biométrie « à trace », en l'occurrence par empreintes digitales[2]. Et le stockage des données n'était pas prévu sur un support individuel mais dans un fichier. Le *dispositif de contrôle d'accès* impliquait donc la conservation par l'employeur, dans une base de données, des empreintes digitales des employés. La CNIL a estimé que rien ne le justifiait. Quant au *dispositif de contrôle des horaires*, il était présenté par une clinique. La CNIL, pour le refuser, a rappelé que si l'objectif d'une meilleure gestion du temps de travail est légitime, il ne justifie pas l'enregistrement dans un lecteur biométrique des gabarits des empreintes digitales des employés.

Géolocalisation

Le 17 novembre 2005, la CNIL avait été amenée à refuser un projet présenté par la MAAF visant à *géolocaliser* de façon permanente les jeunes conducteurs souscrivant une police chez elle.

Le projet concernait une nouvelle offre d'assurance aux jeunes conducteurs qui y auraient souscrit. Chaque jeune conducteur s'engageait, en souscrivant, à respecter un certain nombre de règles parmi lesquelles les limitations de vitesse, un temps de conduite limité (ne pas prendre le volant dans les nuits du samedi, dimanche et jours fériés entre 2 heures et 6 heures du matin).

Pour vérifier le respect des engagements pouvant conduire à une baisse de la surprime appliquée à ces jeunes conducteurs, la MAAF prétendait demander à ceux-ci d'équiper leur véhicule d'un dispositif de géolocalisation de type GPS-GSM. En collectant les informations relatives au déplacement du véhi-

1. Les techniques de contrôle d'accès sont basées sur ce que l'on sait (par exemple un code d'accès), sur ce que l'on possède (par exemple un badge), sur ce que l'on est ou sur une combinaison des trois critères. La biométrie exploite ce que l'on est.
2. Biométrie vient de « bio », vivant et « métrie », fait de mesurer. Un système de contrôle biométrique est un système de reconnaissance des individus à partir de la mesure de leurs caractéristiques vivantes. Les caractéristiques à analyser peuvent être :
   – morphologiques (empreintes digitales, formes de la main, traits du visage…) ;
   – biologiques, à partir de traces (odeur, salive, ADN…) ;
   – comportementales (dynamique du tracé de la signature, frappe sur un clavier d'ordinateur…).

cule toutes les 2 minutes, ce dispositif et le traitement qui devait lui être associé auraient permis à la compagnie de déterminer en permanence la localisation du véhicule, les vitesses pratiquées, le type de route sur lequel roulait le véhicule, ainsi que les horaires et les durées de conduite.

La CNIL a refusé d'autoriser ce traitement pour deux raisons. En premier lieu elle a dit que le traitement qui a pour objet de collecter systématiquement les vitesses maximales pour les comparer aux vitesses autorisées porte sur des *données relatives aux infractions*, à savoir les éventuels dépassements de vitesse. Or l'article 9 de la loi du 6 janvier 1978 interdit aux personnes privées de faire de tels traitements. En second lieu la CNIL a dit que la mise en œuvre du traitement permettant d'enregistrer l'intégralité des déplacements effectués par les assurés est une *atteinte à la liberté d'aller et venir anonymement* qui ne peut être justifiée par la nécessité de contrôler le respect par l'assuré de ses engagements.

Échantillon de patronymes juifs

Le 2 février 2006 la CNIL a refusé d'autoriser un sondage que devait effectuer la SOFRES à la demande du Conseil Représentatif des Institutions Juives de France (CRIF). Il s'agissait d'un sondage d'opinion par téléphone dont l'échantillon devait être constitué par un tri sur les patronymes. La méthode de constitution de l'échantillon consistait à 1. identifier 15 noms à consonance juive sur la base du *Guide des patronymes juifs* édité par Actes Sud ; 2. sélectionner de manière aléatoire 1500 personnes portant un des patronymes parmi les abonnés du téléphone 3. Trier un échantillon de 500 personnes parmi les 1500.

La CNIL a refusé. Elle a dit que la constitution de l'échantillon reposait uniquement sur un tri par le nom. Par conséquent elle était contraire à l'article 8 de la loi du 6 janvier 1978 qui *interdit la collecte ou le traitement de données faisant apparaître directement ou indirectement les origines raciales ou, ethniques ou les appartenances religieuses*.

Vérifications nécessaires

Constitution de fichiers privés d'empreintes digitales du personnel, constatation et sanction privée d'infractions pénales, atteinte à la liberté d'aller et venir anonymement, échantillon de sondage bâti sur la consonance juive des noms... la loi sur l'informatique, les fichiers et les libertés semble avoir de beaux jours devant elle. Sous les mots mesurés de la CNIL, la réalité est bien là.

Les progrès technologiques en croissance exponentielle semblent nourrir chez les personnes privées des volontés de contrôler leurs semblables qui confinent au fantasme. Est-ce à dire que l'État se montre plus raisonnable ?

Mal fichés

Parmi ses attributions, la CNIL est également chargée de jouer les intermédiaires pour l'exercice par les personnes du *droit d'accès indirect*. Elle effectue alors ce que la loi appelle pudiquement les « vérifications nécessaires ». À ce titre, ses commissaires font des recherches dans les grands fichiers de police quand des particuliers pensent avoir été fichés à tort. Et ce qu'ils trouvent là n'est guère plus rassurant. En 2004, à la suite de leurs interventions, pas moins de 1241742 fiches ont pu être éliminées : elles concernaient des personnes mises en cause à tort dans le STIC. En 2005, les demandes de particuliers au titre du droit d'accès indirect ont amené 2513 vérifications dans les divers fichiers du ministère de l'Intérieur. Les investigations dans les fichiers de police judiciaire STIC et JUDEX (fichier de la gendarmerie) ont conduit la CNIL à rectifier les choses dans 44 % des cas. Des fiches obsolètes ont dû être mises à jour. D'autres ont carrément dû être supprimées. Motif : erreur de signalement du fiché ou dépassement de la durée de conservation de la fiche.

Refus d'embauche

Il ne s'agit pas de pures questions de principe. Les fichiers de police sont désormais consultés à des fins qui ne correspondent pas à leur finalité. Des recherches y sont faites à l'occasion d'enquêtes administratives préalables à l'embauche dans certaines professions. Et des gens se voient refuser une embauche ou sont licenciés pour cause de fichage au STIC.

Ils saisissent alors la CNIL pour qu'elle exerce leur droit d'accès indirect. Mais si la réparation de l'erreur intervient dans le fichier, l'emploi, lui, est perdu.

Voici plusieurs années que la CNIL dénonce, comme étant une de ses préoccupations majeures, cette *dérive* de l'utilisation administrative des fichiers de police. On leur fait jouer, dit-elle, un rôle de *casiers judiciaires parallèles* mais sans les garanties du casier judiciaire officiel. Les extraits de celui-ci ne portent, en effet, pas la mention de certaines condamnations pour permettre la réinsertion ou le droit à l'oubli. Rien de tel avec la consultation administrative du STIC. Un signalement sur une fiche et c'est l'exclusion d'un emploi

ou d'une fonction. Or combien de personnes sont fichées au STIC ? En 2004 : cinq millions de mis en cause et dix-huit millions de victimes. Si vous avez un jour été partie civile, vous y êtes !

Fichiers en fiches

Le STIC n'est pas le seul grand fichier public à créer des soucis à la CNIL. Le vieux fichier des RG avec ses quatre millions et demi de fichés[1] est également l'objet de ses incursions au titre du droit d'accès indirect. Comme l'est le plus récent N-SIS, le système d'information de l'espace Schengen avec un million trois cent mille noms qui sont trop souvent à l'origine de refus de visa ou de passeport. Il y a aussi le FIJAIS, fichier judiciaire automatisé des auteurs d'infractions sexuelles (30 000 membres) ou encore le FNAEG, Fichier national automatisé des empreintes génétiques (200 000 profils) qui tend progressivement à supplanter le FAED, Fichier automatisé des empreintes digitales (2 517 000 fiches enregistrées en 20 ans[2]). Sans compter tous les fichiers du ministère de l'Intérieur (fichiers de la PJ, de la Sécurité publique, de la DST, de la Direction centrale de la Sécurité du CEA) et ceux du ministère de la Défense (JUDEX, le fichier judiciaire de la gendarmerie, le fichier de la Direction de la Protection et de la Sécurité de la Défense, celui de la DGSE...). Pourtant, les dangers pour les libertés ne viennent pas des seuls fichiers policiers.

Tour de France

Grande distribution, hôtellerie, télémarketing, *spam*, biométrie, banque... Utilisant ses pouvoirs de sanction, la CNIL, en 2005, a dû adresser 58 mises en demeure pour protéger la vie privée en danger. Un rapide tour d'horizon sur le terrain de ses interventions en dit long sur la « société des fichiers » et ses menaces.

Harcèlement

Ainsi, dans le secteur de l'hôtellerie, un contrôle sur place a révélé chez un groupe leader en Europe des listes de clients à risques annotées de commentaires comme « droguée, sale, fume chichon, fille arabe, manouche, tête de

1. Au 1er janvier 2006.
2. Le nombre des affaires « résolues » au stade policier grâce au FAED serait passé de 577, en 1993, à 7 300 en 2006. Le nombre des affaires « rapprochées » grâce au FNAEG serait passé de 19, en 2002, à 5 741 en 2006 (source : *Bulletin mensuel de l'Observatoire national de la délinquance*, mars 2007).