CHAPITRE 1
ÉLOGE DE L'INTIMITÉ

Dans le film *The Truman Show*, l'acteur Jim Carrey campe un personnage, Truman Burbank, dont les faits et gestes quotidiens sont filmés, enregistrés et diffusés en permanence, et cela, depuis sa naissance. Le personnage principal mène une existence simple et sans histoire, constituée des multiples événements anodins de la vie quotidienne. Son mode de vie, proche du nôtre, nous permet de nous identifier à lui : aussi ressentons-nous avec lui le malaise grandissant que le réalisateur, Peter Weir, instille avec subtilité. Œuvre de fiction, cette histoire pose avec humour de nombreuses questions concernant le respect de l'intimité. La diffusion du show sur les grands réseaux de télévision donne un impact supplémentaire aux propos du cinéaste mais l'inquiétude ressentie ne se borne pas à une question quantitative. À la place de Truman Burbank, serions-nous vraiment moins troublés si une seule personne, plutôt que quelques millions, épiait nos faits et gestes ? Serions-nous plus sereins si cette surveillance se limitait à un seul aspect de notre vie quotidienne : nos déplacements par exemple, ou notre santé, ou encore notre correspondance ?

Avec le développement des technologies de l'information et de la communication, la réalité est en passe de rattraper la fiction. Depuis les systèmes de vidéosurveillance des voies et espaces publics jusqu'aux réseaux de localisation par satellite en passant par la

téléphonie mobile et les nombreuses cartes à puces dont nous faisons un usage quotidien, les technologies actuelles ouvrent de nouvelles perspectives – quasi infinies – dans ce domaine.
Ces outils facilitent notre vie quotidienne. Conçus pour nous aider, pour simplifier nos achats, nos déplacements, nos démarches administratives, pour nous rapprocher les uns des autres malgré les distances, ils portent souvent en germe un risque potentiel pour nos libertés en fournissant de nombreux renseignements sur notre personnalité et sur nos activités. Depuis sa création en 1978, plus d'un million de fichiers nominatifs ont été déclarés à la CNIL[1] et ce nombre augmente d'environ 100 000 chaque année. Selon certaines sources, il y aurait en réalité dix millions de fichiers nominatifs en France et le nom de chacun d'entre nous figurerait dans plusieurs centaines de fichiers différents. Il n'est guère de composantes de notre vie quotidienne qui échappe au quadrillage du monde numérique : mouvements bancaires, situation fiscale, traitements médicaux, déplacements, achats, appels téléphoniques, courriers électroniques, etc. Tout, ou presque, y passe.
Enregistrés en permanence et de façon entièrement automatisée pour les nécessités du service, ces renseignements, parcellaires et dispersés, dorment le plus souvent dans les gigantesques mémoires d'ordinateurs. Mais si ces données devaient être un jour mises en commun et conservées, elles tisseraient un étroit maillage de notre sphère personnelle, permettraient une traçabilité complète de chaque individu, mettant ainsi en réel danger nos droits fondamentaux. Nos gouvernants et les grands groupes industriels sauront-ils résister à la tentation d'utiliser à leur profit la mine quasi inépuisable d'informations qu'ils ont à leur portée, presque gratuitement ? Et que resterait-il de notre intimité si un gouvernement ou une grande société commerciale s'avisait de les réveiller, les regrouper, les classer, les archiver et les exploiter ?

---

[1] CNIL : *Commission Nationale de l'Informatique et des Libertés.* La Commission définit ainsi son rôle : « *La mission générale de la CNIL est de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.* » (www.cnil.fr)

Il faut ici souligner que, même anonyme, une information peut potentiellement porter atteinte à la vie privée. À juste titre la CNIL définit comme une « *donnée à caractère personnel* » « *toute information relative à une personne physique identifiée ou susceptible de l'être, directement ou indirectement* »... même si celle-ci n'est pas nominative. La CNIL donne sur son site Internet[2] plusieurs exemples d'information à caractère personnel : « *"le titulaire du numéro de ligne 0153732200 téléphone souvent au Sénégal" ou "le propriétaire du véhicule 3636AB75 est abonné à telle revue" ou encore "l'assuré 1600530189196 va chez le médecin plus d'une fois par mois".* » Il est clair dès lors que la mise en commun de plusieurs fichiers ne contenant aucune information nominative peut, grâce à des recoupements, déboucher sur un fichier personnel très documenté. Que dire alors d'un fichier unique compilant, pour chaque femme, chaque homme, chaque enfant résidant en France, toutes les données pour le moment éparpillées dans quelques 500 fichiers distincts ?

On peut bien entendu objecter qu'une telle compilation n'est pas à l'ordre du jour et que, en outre, elle serait techniquement difficile à réaliser. C'est probablement vrai... pourtant des projets similaires, plus modestes, refont périodiquement surface. Le projet *Safari* prévoyait par exemple, dans les années 1970, d'identifier chaque citoyen par un numéro unique et d'interconnecter sur la base de cet identifiant tous les fichiers de l'administration[3]. Plus récemment, certains parlementaires, adeptes du tout numérique, ont proposé « pour nous simplifier la vie » de regrouper carte d'identité, carte de paiement, carte d'électeur, permis de conduire, carte de santé, dossier fiscal... en une carte à puce unique. Est-ce bien raisonnable ?

Quoi qu'il en soit, les fichiers existants se nourrissent, dans une certaine mesure, de ce que chacun d'entre nous veut bien leur fournir. À cet égard, un tour d'horizon – non exhaustif – de ce que

---

[2] www.cnil.fr : « *La CNIL en bref.* »

[3] Face aux inquiétudes que ce projet suscita dans l'opinion publique, le gouvernement se vit contraint de mettre en place une commission qui, entre autres, proposa la création d'une autorité indépendante, donnant ainsi naissance à la CNIL.

permet la technologie actuelle, lorsqu'elle s'allie à notre négligence, est instructif.

• *Courrier électronique*

Extrêmement vulnérable, il transite d'un ordinateur à l'autre en passant par de nombreux intermédiaires. De façon générale, tout document entrant ou sortant de notre ordinateur peut être intercepté, toute information dormant dans notre disque dur peut être détournée, si l'un et l'autre ne sont pas protégés efficacement. Ainsi, fournisseurs d'accès, serveurs (dans les réseaux internes d'une entreprise ou d'une université) et bien d'autres personnes physiques ou morales peuvent – techniquement – lire « à livre ouvert » notre courrier, nos contributions aux forums de discussion, connaître les sites que nous visitons et la teneur des documents que nous chargeons... Une simple possibilité qui pourrait bientôt devenir une obligation légale dans l'Union européenne. Selon l'hebdomadaire *Courrier International*[4] :

> « *Le projet [des ministres européens de la justice] est de stocker toutes les données relatives aux courriers électronique, à la navigation et aux forums de discussion pendant une durée allant de un à trois ans. [...] C'est de cette proposition qu'il a été question [...] le 14 avril [2005] entre les ministres européens de la Justice et de l'Intérieur à Bruxelles.* »

En d'autres pays, ces dispositions sont déjà effectives[5] :

> « *A partir du 31 juillet 2005, les fournisseurs d'accès à Internet argentins devront stocker les déplacements sur la toile de tous leurs clients pour une période de dix années [...]. Dès lors, chacun des sites visités, les courriels envoyés ou reçus ainsi que le contenu des chats*[6] *seront consignés et laissés à la disposition des services de renseignement et de la justice qui pourront en faire la demande.* »

• *Technologie sans-fil*

---

[4] *Courrier International*, 12 mai 2005. L'hebdomadaire reproduit un article de Michael Persson et Jeroen Trommelen paru dans le quotidien *De Volkskrant* (Pays-Bas).

[5] *Courrier International*, 12 mai 2005.

[6] Il s'agit de la « messagerie instantanée », en plein développement sur Internet : un groupe d'internautes se retrouve sur le réseau pour discuter en direct par messagerie électronique. Le mot anglais « chat » signifie « causerie », « discussion ».

La technologie « Wi-Fi » permet de relier entre eux ordinateurs, imprimantes, modems... en s'affranchissant des câbles de jonction. Les échanges se font par liaison radio... malheureusement les ondes électromagnétiques ne s'arrêtent pas aux murs de notre bureau ou de notre appartement ! Si nous sommes négligents, le contenu de nos disques durs est à la merci d'un pirate opérant à partir d'un véhicule avec un simple ordinateur portable. La *Commission Nationale de l'Informatique et des Libertés* estime[7] :

> « *La confidentialité des informations traitées par les équipements et réseaux Wi-Fi étant encore insuffisante, la CNIL recommande aux utilisateurs et professionnels de ne pas les utiliser sans précautions particulières.* »

• *Indexation des disques durs*

Des logiciels gratuits permettent de référencer dans un moteur de recherche la totalité des documents contenus dans un disque dur personnel. Avantage ? Si vous avez oublié l'emplacement d'un document dont vous avez seulement un vague souvenir, il vous suffira de taper quelques mots-clés sur votre moteur de recherche pour le voir apparaître en tête de liste. Bien entendu, nul n'est tenu de livrer ainsi l'ensemble de ses travaux personnels à quelques serveurs lointains. Certaines firmes informatiques prévoient pourtant – rêve ou cauchemar ? – la disparition de l'ordinateur personnel que nous connaissons au profit d'un simple terminal dépourvu de mémoire de masse qui nous mettrait en relation avec nos données personnelles, stockées à distance.

• *Téléphone portable*

Pour les associations de défense des libertés individuelles, les téléphones portables génèrent deux risques très différents : la géo-localisatio – qui échappe aux ressources de la cryptologie – et l'interception des communications. Conformément à la loi, les opérateurs de téléphonie doivent conserver toute information concernant la localisation de chacun de leurs abonnés (environ 45 millions en France), les dates, heures, durées de tous les appels entrants et sortants ainsi que l'identité de leurs correspondants et ce,

---

[7] www.cnil.fr

durant plusieurs mois[8]. Par ailleurs, avec du matériel, relativement onéreux certes, disponible auprès d'officines privées spécialisées, il est possible d'écouter toutes les conversations téléphoniques de proximité. Chacun connaît l'orientation des prix, en baisse constante, dans les domaines de l'informatique et de l'électronique : on peut donc craindre un fort développement du marché de « l'écoute téléphonique » privée, comparable à celui que connaît déjà le secteur des microphones et des caméras miniatures.

La cryptographie, pourquoi ?

Il y a environ cent cinquante ans, personne ne pouvait écouter votre conversation sans que vous le sachiez. Si une oreille indiscrète s'approchait de vous, vous pouviez vous éloigner et reprendre ailleurs votre discussion. Le droit à la vie privée était ainsi garanti par les lois de la physique sans qu'il soit nécessaire de légiférer. Avec le téléphone, cette protection naturelle a disparu : la possibilité de converser à distance s'est accompagnée de la possibilité d'écouter les conversations d'autrui, à distance et à leur insu. Très vite des abus se sont installés et, sous la pression des citoyens, les hommes politiques ont dû encadrer ces pratiques. Mais un pas était franchi : désormais le respect de l'intimité et de la vie privée n'allait plus de soi. Les grandes démocraties ont donc inscrit dans la loi de nouveaux droits assurant la protection des citoyens.

Les garanties individuelles sont ainsi clairement exposées. La Déclaration universelle des droits de l'homme, adoptée par l'Assemblée générale des Nations unies le 10 décembre 1948, stipule par exemple, en son article 12 :

> « *Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à*

---

[8] Pour rentabiliser leurs équipements... et financer leurs obligations légales de conservation des données, les opérateurs souhaitent pouvoir céder une partie de ces informations à leurs abonnés, moyennant abonnement. Au Japon et en Grande-Bretagne, ces services complémentaires sont déjà disponibles auprès du grand public : ils permettent à des parents, par exemple, de localiser avec précision leurs enfants. En France, plusieurs sociétés commercialisent ce type de services auprès des entreprises. La CNIL étudie actuellement les modalités pratiques de leurs extensions éventuelles à l'ensemble des abonnés.

son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes ».

La Convention européenne des droits de l'homme va dans le même sens (Article 8, alinéa 1) :

« *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.* »

Cependant l'évolution technique est si rapide que le législateur peine souvent à adapter la loi et à la faire respecter efficacement. Les enjeux économiques, considérables, et les nécessaires impératifs de sécurité limitent en outre la capacité d'intervention des pouvoirs publics, laissant parfois s'installer des vides juridiques inquiétants. En proposant au grand public des méthodes efficaces pour se prémunir de toute indiscrétion dans le respect de la loi, la cryptographie moderne soulage la puissance publique d'une charge qui est de plus en plus difficile à assumer.

Le simple particulier n'a guère de prise sur la plupart des risques évoqués plus haut. Sauf par son vote – lorsqu'on lui demande son avis – ou par son action militante, il ne peut pas facilement aller à l'encontre des mesures sécuritaires prises par les gouvernements ou à l'encontre de la stratégie agressive de certaines firmes commerciales. À défaut, il peut tout au moins limiter la « fuite » d'informations le concernant et ne pas nourrir inconsidérément l'avidité des prédateurs qui le guettent.

La cryptographie a pour but de garantir et de préserver la confidentialité de notre correspondance. Elle protège de toute immixtion aussi bien notre courrier électronique que nos conversations téléphoniques. Plus généralement, elle empêche, en cas d'intrusion, de perte ou de vol, la lecture de tout document numérique archivé dans nos ordinateurs ou sur un support externe. Elle a donc vocation à protéger efficacement textes, photos, enregistrements sonores ou vidéos, conversations téléphoniques… Dans cet ouvrage nous examinerons les principes et les moyens mis en œuvre pour atteindre cet objectif.

Mais avant, la question demeure : la cryptographie, pourquoi ?

Si nous acceptons tous, comme un fait acquis, que des secrets vitaux dans les domaines militaires, diplomatiques ou économiques soient coûte que coûte préservés, nous n'éprouvons pas nécessairement le besoin de protéger notre propre correspondance : si je n'ai *rien* à cacher, pourquoi devrais-je *tout* cacher ? Pour répondre à cette question, il est nécessaire d'insister sur une caractéristique particulière des échanges numériques.

Si le courrier électronique présente d'indéniables avantages sur le courrier postal, il ne faut pas oublier une différence essentielle : l'extrême vulnérabilité du premier par rapport au second.

Détourner une lettre confiée par son expéditeur aux services postaux, l'ouvrir, en prendre connaissance, la refermer et la remettre dans le circuit sans éveiller l'attention demande des moyens techniques, humains et financiers importants. Tout cela suffit pour mettre les correspondances postales de la majorité d'entre nous à l'abri des tentations de nos gouvernants ou de notre voisinage. Il en va de même de nos conversations téléphoniques : installer une dérivation sur une ligne analogique, la mettre sur écoute, engager du personnel pour pratiquer la surveillance et faire une synthèse des communications passées, etc. coûte cher, ce qui met également les citoyens ordinaires à l'abri de tout abus en ce domaine.

Avec les moyens informatiques modernes, les mêmes violations de la vie privée peuvent être réalisées pour un coût dérisoire et souvent sans intervention humaine. Des ordinateurs spécialisés peuvent se charger de lire, écouter, trier, mettre en mémoire et analyser toutes sortes d'informations[9].

L'histoire montre que, de tous temps, en tous lieux, les États se sont accordé le droit de surveiller leurs ressortissants. Les démocraties ne sont pas en reste dans ce domaine et la tentation d'aller au-delà

---

[9] Le réseau « *Échelon* » mis en place par les États-Unis, avec l'aide de la Grande-Bretagne, du Canada, de l'Australie et de la Nouvelle Zélande, capte, analyse et trie systématiquement tous les échanges numériques transitant par satellites : fax, courriers numériques, communications téléphoniques, etc. Lire à ce propos les articles de Philippe Rivière « *Tous les européens sur écoute* » et « *Grandes oreilles américaines* » dans *Le Monde Diplomatique*, mars 1999. Des dispositifs analogues se chargent des communications véhiculées par les câbles sous-marins : lire à ce sujet *Surveillance électronique planétaire*, Duncan Campbell, Éditions Allia, Paris, 2003.