CHAPITRE 6

La culture proprement européenne au sein de la culture occidentale

Raymond POLIN

Ce texte a été rédigé en 1999, par l'auteur, sous forme de communication au groupe «Société d'information et vie privée» et à sa demande. Le groupe souhaitait une réflexion de base permettant de mieux comprendre la différence entre les notions de vie privée en Europe et aux États-Unis, et surtout entre les principes orientant les solutions de protection de la vie privée. Raymond Polin situe ce besoin de vie privée dans l'exercice des libertés et dans la dignité humaine, qui sont dans la tradition de l'humanisme occidental.

Depuis trente siècles se sont accumulées, venant des lointaines régions de l'Est, dans cette petite péninsule hirsute extrême-occidentale de l'Asie, ces populations qui ont progressivement formé l'Europe de nos jours, une Europe entourée de mers, dont les frontières terrestres s'étendent à l'est plus ou moins aussi loin que la religion chrétienne, jusqu'aux territoires où règne la religion orthodoxe.

Car l'Europe est d'abord, jusqu'à nos jours, une culture constituée par des valeurs judéo- chrétiennes, appelée par des valeurs grecques, modelée, transmise, par des valeurs romaines, influencée par le droit romain et par des traditions germaniques. Cette culture européenne commune est mise en œuvre, dans sa longue histoire, par des communautés politiques aux sous- cultures originales, exprimées dans plusieurs langues d'origine essentiellement indo- européenne, et par des mœurs, par des coutumes, par des œuvres et des arts qui sont propres à chacune d'entre elles, mais qui, toutes, expriment à leur façon cette culture européenne majeure dans une sorte d'œcuménisme culturel, une culture qui exprime fondamentalement une certaine conception de l'homme, un humanisme. Depuis deux ou trois siècles, des communautés politiques ont formé des nations, et ont ainsi pris conscience et affirmé politiquement, leurs propres cultures nationales.

Et que je le dise en passant, les Etats-nations sont le chef-d'œuvre tardivement accompli par la culture de l'Occident. Les États-nations sont essentiels à l'existence d'une Union européenne, à deux conditions : la première, c'est qu'on les défende contre une exploitation fâcheuse sous la forme de nationalismes agressifs ou contre une tentation d'impérialisme dominateur, reliquats d'une histoire encore récente. Mais, en second lieu et tout autant, il importe de défendre le concept et l'existence d'États-nations en Europe contre des idéologies destructrices de la nation, lorsque certains s'efforcent de les dissocier et de leur substituer, au nom d'infrastructures plus ou moins folkloriques, des communautés internes, qui vivraient plus authentiquement sur un plan social que sur un plan politique, ce qui les rendrait incapables d'exister comme des communautés autarciques, ce qui les empêcherait, du même coup, d'être composées d'authentiques citoyens.

Dans leurs constantes communications, dans leurs luttes comme dans leurs coopérations, les cultures mineures nationales et la culture majeure proprement européenne se développent et s'affirment dans la participation à une même histoire qui est essentielle à l'existence de l'homme européen, comme aux sujets, ou aux citoyens de chacune de ces nations qui vivent de cette histoire. Les Européens sont des hommes culturels, des hommes historiques pour qui importe essentiellement la mémoire de leur passé, condition de l'entreprise de leur avenir, un avenir humaniste.

Les valeurs qui dominent et orientent la culture européenne historique s'imposent aisément à notre analyse, à condition, bien sûr, de ne prendre en considération que les valeurs classiques, immuablement fondamentales, en dépit des révoltes ou des crises temporaires qu'elles peuvent subir.

Et d'abord, par excellence, la valeur de liberté, qui permet à chaque homme d'aller au-delà de sa nature donnée, de se transcender indéfiniment lui-même, précisément dans une histoire, qui fait de l'homme un être qui se fait, qui est pour l'essentiel sa propre œuvre. Mais, surtout, que l'on ne confonde pas la liberté avec l'arbitraire, la licence, la gratuité, le « tout est permis ». Le propre de la liberté, c'est d'avoir une fin, d'avoir du sens, un sens compréhensible et justifiable : bref, le propre de la liberté, c'est d'être une liberté raisonnable, mettant en œuvre des valeurs raisonnables.

Et cela va de soi : car la forme la plus primitive de la liberté, c'est la réflexion, qui va au-delà d'elle-même, qui, en réfléchissant, se donne du sens.

Kant avait bien vu le paradoxe, qui établit un rapport essentiel entre la liberté et l'art de raisonner, de chercher le raisonnable (c'est le passage non moins essentiel de la réflexion raisonnable, de la compréhension de l'humain et de ses valeurs, à la théorie rationnelle, à la formation d'un savoir, qui offusquera ce rapport premier de la liberté à la raison en le présentant comme apparemment peu vraisemblable).

On a tôt fait de s'apercevoir que si réfléchir, c'est essayer de se comprendre, comprendre tout court, c'est aussi essayer de se faire comprendre par l'autre homme, par d'autres hommes. Et même que l'on se comprend d'autant mieux que l'on connaît la façon dont tel autre, dont les autres vous comprennent. La réflexion, la conscience de soi, est inséparable de la conscience pour l'autre et par l'autre.

Nous sommes ainsi amenés à conclure de cette réciprocité qu'il y a égalité entre les hommes, étant bien entendu qu'il s'agit d'une égalité d'essence, d'une capacité de liberté, d'une capacité de conscience réfléchie et raisonnable, mais non pas d'une égalité en nature, d'une égalité en acte.

Car la liberté et l'égalité sont pour ainsi dire des sœurs, mais des sœurs ennemies, la liberté étant un principe irréductible de différence, de divergence, d'originalité. Les hommes sont des êtres semblables, en ce sens qu'ils appartiennent tous à une espèce unique, mais ils sont tous individuellement distincts et différents. C'est donc un contresens grave que d'essayer, contre leur nature, de les rendre effectivement égaux et de les conformer à un type unique, d'en faire des êtres homogènes. L'égalité compatible avec la liberté, et qui est seule capable d'assigner à cette liberté des limites raisonnables, c'est l'égalité de droit, l'égalité des droits au sein de la communauté que forme un ensemble d'individus humains et qui, de ce fait, devient une communauté politique nécessairement régie par une autorité publique.

Nous parachevons ainsi la définition de l'humanisme que nous défendons en reconnaissant que l'homme est un être social et, mieux encore, comme le disait Aristote, un animal politique.

Tâchons de mettre en évidence quelques caractères, quelques manifestations de cet humanisme historique bien européen.

Il faut reconnaître sa complexité et les problèmes qu'elle suscite. Il n'est pas facile de réussir à accomplir chacun pour soi ou pour l'ensemble d'une communauté politique, son humanité.

Ces trois pôles de l'existence des hommes que nous avons soulignés, individualisme requérant autonomie et indépendance, égalité des droits sur laquelle pèse l'obsession d'une égalité des avantages effectivement reçus et vécus, existence politique, ne sont pas en harmonie immédiate. Les conflits qu'ils entretiennent marquent la finitude de l'homme et son irréductible imperfection. Le principe de sa liberté, sa capacité d'aller au-delà de lui- même, en qui tous ses espoirs de perfectionnement reposent, forment aussi bien le principe de son imperfection. C'est le principe moral fondamental du christianisme. L'homme est capable du meilleur ou du pire, et même du meilleur *et* du pire. Il est, par essence, puisqu'il est libre, interdit de perfection.

La liberté d'expression qui nous intéresse ici tout particulièrement concerne la liberté d'opiner, la liberté des opinions. Dans l'histoire de l'Europe, elle a été fort longtemps limitée par des dogmes, religieux ou philosophiques, que l'Église ou la puissance publique faisaient impérieusement respecter. Ce n'est guère qu'au XVIIIe siècle que s'est installée en Europe une liberté d'expression qui s'est progressivement affirmée en théorie et en acte avec la philosophie des Lumières, développée en particulier à partir des œuvres de John Locke. Les disciples américains des philosophes des Lumières et les philosophes européens ont repris et appliqué à la liberté d'expression la vieille maxime romaine, dite de droit naturel « Ne fais pas à autrui ce que tu ne voudrais pas qu'il te fit », *alteri ne feceris quod tibi feci non vis.* En l'appliquant à la liberté de penser, de croire et de s'exprimer par quelque procédé que ce soit, les *Founding Fathers* américains sont allés plus loin encore en refusant quelque limite que ce soit à la liberté d'expression, comme l'indique le Ier Amendement du *Bill of Rights.* Cette option donne lieu à d'évidents excès. Le dévergondage médiatique, les laxismes de la bioéthique sont de nos jours la preuve de ces ravages dans l'Occident américain.

En revanche, il ne faut pas oublier que la liberté est d'abord un pouvoir; elle n'est pas immédiatement un droit, et c'est seulement entre les droits que l'égalité entraîne nécessairement leur limitation réciproque. Nietszche a fait remarquer que, si la liberté d'expression de l'un était rigoureusement limitée par le respect de la liberté d'expression de l'autre, toute discussion allant au fond des choses, et même toute conversation destinée à avoir des conséquences pratiques, serait pratiquement interdite. Ce qui serait fâcheux et même absurde.

La Déclaration française des droits de l'homme et du citoyen, qui rassemble manifestement de nos jours les convictions les plus ardentes relevant de la culture européenne, ne va pas si loin. Elle ne se contente pas d'un appel au respect réciproque de la liberté d'expression entre citoyens raisonnables, à la relation essentielle de ces droits à des devoirs, elle donne à la loi la tâche de transformer ce pouvoir en droit, dans toute la mesure où cela est nécessaire. C'est, en effet, seul l'État qui peut dire le droit, même dans les pays coutumiers. Et, ici encore, cette méthode de définition de la liberté d'expression ne va pas sans de graves dangers. L'État dit le droit, mais il n'est pas apte à dire le vrai, et s'il prétend proclamer telles opinions comme vraies et interdire telles autres comme fausses, il entre dans la voie du despotisme. Les régimes totalitaires récents nous ont mis en présence des catastrophes qui se sont ensuivies.

J'en profite pour signaler, chemin faisant, qu'à une époque récente certains groupes de pression se sont arrogé le droit de faire intrusion dans les opinions d'autrui et d'en interdire l'expression sous prétexte qu'elles seraient « politiquement incorrectes ». Tous les moyens leur sont bons, la mise en garde, l'organisation du silence, bref la violence spirituelle, et parfois la violence physique. Il va sans dire qu'il s'agit là d'opérations idéologiques injustifiables et intolérables.

Laissons ici le problème des recherches scientifiques et des divers types de vérités qu'elles sont, suivant leur nature, en mesure d'établir. Les opinions qui sont l'objet ordinaire de la liberté d'expression ne sont que des manières de penser et de croire. Elles ne relèvent pas de l'ordre des vérités, elles expriment les apparences du monde dans lequel nous pensons, nous vivons, nous agissons. A leur propos, il ne peut s'agir que d'un degré de créance, d'un degré de sincérité ; elles relèvent de l'ordre des valeurs. Les limites que nous pouvons imposer à l'expression d'une opinion sont d'ordre moral et dépendent de la nature de ceux auxquels nous les exprimons et de la considération, du respect que nous leur portons.

Comme l'avait déjà signalé Montesquieu, les lois ne suffisent pas pour imposer ou même pour corriger les mœurs. En dernier ressort, il faut invoquer des valeurs morales, seules capables à la fois d'être générales et de s'appliquer à des cas particuliers. Il s'ensuit qu'il convient ici, singulièrement dans nos démocraties libérales, de réclamer l'usage de la vertu, des vertus fondamentales, comme la seule solution possible de ce problème grave, plus encore chez les gouvernants que chez les gouvernés.

Nous n'aurions pas fait le tour complet du problème de la liberté d'expression, cette valeur essentielle, si nous ne signalions pas cette forme particulière qu'elle prend, fort insidieusement, et qui tient une si grande place dans nos vies personnelles, ce que la culture occidentale américaine pratique si mal et qui porte cependant si bien un nom anglo-saxon, la *privacy*, le respect rigoureux de la vie personnelle intime, de la vie privée. Elle est pourtant le foyer le plus actif, le plus créateur de la réflexion individuelle et de la formation de la personne, de son œuvre, le principe et la source de sa dignité.

La *privacy* est un tout très intime, très secret et même pour soi-même, et évidemment très confidentiel. C'est le for intérieur, qui est la réflexion en acte, dans sa gestation, dans ses incertitudes, qui est, pour ainsi dire, au cœur de soi-même. Le for intérieur est le domaine de l'incertain d'où peut sortir la certitude, et, cette expression banale le dit bien, si l'on donne un sens plénier aux mots qui la composent, lorsque l'on parle de « en son âme et conscience », même si l'on n'est pas sûr d'avoir une âme et si l'on ne sait pas bien en quoi consiste, en ses sens multiples imbriqués, la conscience, conscience psychologique ou conscience morale, l'immortelle et céleste voix de Jean-Jacques Rousseau. Pendant sa longue gestation, c'est, ce peut être jusqu'au bout, l'indicible. Faire intrusion dans ce for intérieur, c'est, à la limite, absurde et impossible ; c'est en tout cas une forme inhumaine d'expression autour de laquelle rôdent la violence spirituelle et la violence physique.

La *privacy*, c'est aussi la vie privée vécue, les démarches de la vie personnelle qui ne concernent et ne regardent personne, la vie familiale, les amitiés et les amours, qu'on est strictement en droit de ne pas révéler et de garder pour soi seul, sauf s'il s'ensuit des conséquences publiques répréhensibles. On peut y ajouter ses convictions les plus intimes, les opinions les plus secrètes que l'on ne souhaite pas exprimer sans avoir même à se justifier. Toute intrusion, toute exigence venue d'autrui est incongrue et relève, là encore, de la violence, même si c'est un magistrat qui l'exerce. « N'avouez jamais » semble une formule cynique, mais c'est bien la formulation populaire du premier des droits de l'homme qui ait jamais été proclamé, mais oui, c'était par Thomas Hobbes, en 1642, l'affirmation du droit de tout homme à ne pas s'accuser soi-même quoi qu'il ait pu faire, un droit qui sera repris dans le V^{e} Amendement du *Bill of Rights* américain de 1791.

Nous sommes ainsi amenés, tout à l'heure par l'évocation de la justice comme vertu et maintenant par l'appel à la justice comme institution, à esquisser sommairenient la place de la Justice dans l'humanisme occidental — ce qui nous met en présence, sur cet exemple particulier, d'une découverte surprenante, la double et contradictoire tendance de l'humanisme occidental à se

concentrer, dans certains cas, sur le particulier, l'original, l'incomparable, ou, sur d'autres thèmes, à extrapoler vers l'universel.

Ce qui va provoquer des divergences, parfois en sens contraire, entre la culture européenne, cultivée sous une forme œcuménique, à travers le passé historique des vieilles nations d'Europe, et la culture occidentale américaine, qui n'a d'autre passé que les religions protestantes apportées par les émigrants anglo-saxons en Amérique et l'héritage philosophique des Anglais et des Français des Lumières, transformés en institutions politiques à vertus éducatives définitives par les *Founding Fathers,* et inscrits par eux dans la Déclaration d'indépendance de 1776, ou dans la Constitution de 1788, dans le *Bill of Rights* de 1791.

Alors qu'en Europe l'influence du droit romain, tout en intégrant certaines coutumes venues des communautés germaniques, reste prépondérante, que l'autorité de l'État et de la loi aboutit aux mêmes décisions sur toute l'étendue du territoire, que la jurisprudence n'intervient que pour adapter la règle aux circonstances, que l'élaboration de codes apparaît comme un progrès évident et nécessaire, aux Etats-Unis, l'exemple anglo-saxon triomphant, la procédure des contrats l'emporte sur celle de la loi qui n'est jamais qu'une *soft law*, la justice est rendue en fonction des cas retenus par une jurisprudence dominatrice et, dans l'État fédéral, les décisions de justice dépendent de la jurisprudence constatée dans chaque État de la Fédération pris en particulier. Ici, les procès suivent une procédure inquisitoire où le juge applique la loi ; là, ils suivent une procédure accusatoire, et le juge est avant tout, au cours du procès, un arbitre d'une riche expérience, et sa décision définitive, la conclusion d'un arbitrage.

En revanche, et si nous passons de la Justice aux mœurs vécues, aux conditions de vie et de travail, nous constatons que la particularité des cultures locales donne lieu en Europe à un type de réflexion relativement récent qui n'est ni moral ni politique, au sens universel que ces mots peuvent prendre. Cette réflexion développe de nouvelles valeurs de plus en plus bruyamment réclamées, des « valeurs sociales », très différentes des valeurs inspirant la justice politique, évaluant les conditions et les niveaux de vie locaux, donnant lieu à des groupes de pression puissants, à des manifestations mettant en cause l'ordre public et plus encore des exigences et les résultats de l'activité économique et financière. À ces valeurs sociales, on veut faire correspondre des droits réels. Ainsi se constitue progressivement et s'impose, par exemple, une politique des revenus, et l'on veut donner à l'État, par un curieux retour à l'universel et à une centralisation drastique, la charge de l'accomplir. .

Au contraire, aux Etats-Unis, où les *Wasps* ont progressivement perdu de leur autorité, où le *melting pot* et ses quotas est dépassé par l'afflux des populations étrangères non anglophones, certains estiment qu'aux traditions morales et aux exigences politiques en perte de vitesse se substitue une ère des technologies, où des techniques universelles de plus en plus sophistiquées, puissantes et absorbantes prétendent, l'informatique contemporaine aidant, apporter des solutions proprement techniques aux problèmes sociaux et politiques que la morale et la politique traditionnelles ne suffisent plus à résoudre.

Sur l'immense continent (9 400 000 kms²) occupé par les États-Unis d'Amérique, la densité de la population (29 hab./km²) est très faible et cette population (265 millions d'habitants) se trouve tellement concentrée sur d'importantes zones urbaines, situées loin les unes des autres, dans des climats très divers, marquées par une très forte décentralisation, peuplées de populations aux mœurs, aux origines ethniques et même aux langues assez diverses. Au sein d'un fédéralisme réduit à l'essentiel, les Américains ont l'expérience d'une certaine forme de multiculturalisme modéré, tempéré par une circulation très générale à la recherche d'une profession et surtout par le conformisme des manières de vivre engendré par l'usage de techniques qui accaparent les moyens et même bien souvent les fins de la vie domestique, de la vie quotidienne. Peut-être, pour 80 % des habitants, hormis 10 % de très pauvres et 10 % de très riches, ce multiculturalisme est-il plus apparent qu'effectif Mais il suscite chez les Américains de souche l'illusion qu'il faut résoudre les problèmes nationaux de l'Europe, par exemple dans les régions fragiles du Sud-Est, en organisant des États multiculturels. Pensons aux Balkans. C'est dire à quel point il leur manque le sens de l'histoire, de sa permanence dans le présent.

En interprétant des tendances peut-être plus qu'en observant les faits, on peut se demander si la culture européenne qui, depuis deux siècles, avait basculé des deux côtés de l'Atlantique, pour devenir la culture occidentale judéo-chrétienne, gréco-romaine, n'est pas en train, non certes pas de se scinder, mais de marquer des différences. Les distinctions linguistiques mises à part, on peut se demander aussi s'il n'advient pas une différence plus grande entre la culture occidentale européenne et les cultures occidentales d'outre-Atlantique qu'entre deux cultures nationales d'Europe.

Peut-être y a-t-il d'autres raisons à cette différence, surtout lorsque celle-ci risque de susciter une opposition, comme par exemple l'extraordinaire surcroît de puissance politique et militaire riche de tentations, aux États- Unis, ou encore la prodigieuse production industrielle suscitée par les hautes technologies et les

concurrences commerciales que celles-ci suscitent et qui risquent de tourner en relations d'hostilité.

Cependant il me semble que les principales divergences tiennent à l'histoire de ces deux ensembles culturels et à l'impact de la civilisation américaine, C'est-à-dire de la science et de la recherche américaines et des techniques prodigieuses qui s'ensuivent, de l'accélération foudroyante de leurs progrès matériels.

Peut-être aussi, même si les talents intellectuels sont analogues de part et d'autre, les générations européennes, quels que soient les génies et les exploits qu'elles puissent comporter ici et là, courent le risque de se trouver coincées dans les habitudes, les avantages, les règlements reçus du passé, si elles ne cultivent pas suffisamment ce goût de l'innovation, cet appétit d'invention et de découverte, cet esprit d'entreprise et cette hardiesse dans la mise en œuvre qui font du monde systématiquement technique des Américains un monde en constante construction, en constant progrès scientifique et technologique. En dépit, ici et là, de manifestations de ferveur religieuse incontestable, un matérialisme ordinaire risque de s'installer.

Pour faire face à ce déséquilibre, il ne suffit pas que les Européens excellent à créer des valeurs et des œuvres d'une humanité toute spirituelle, capable de rivaliser avec les créations américaines du même ordre et même de les inspirer et de les dominer.

Les Européens, à leur façon, se doivent aussi d'associer à leurs dons créateurs, à leur art de vivre, à la douceur qu'ils sont capables de donner à l'existence dans leur monde humanisé, un engagement pratique, un esprit d'entreprise, une volonté d'accomplissement, qui leur permettront alors de prendre efficacement leur juste part de l'œuvre américaine, sans quoi ils risqueraient de se trouver dominés par l'immensité des activités techniques de la civilisation américaine qu'ils ne parviendraient plus à maîtriser et même à comprendre. Comme l'inondation informatique ne comporte pas, par nature, d'ordre interne — l'ordre est le signe de l'humanité — et comme elle ne supporte aucun contrôle extérieur, elle risque de substituer l'information brute à la connaissance réfléchie. Aux Européens de contribuer à dominer ce mondialisme technique envahissant, de l'ordonner et de le subordonner à des recherches de sens et de valeurs.

En revanche, plus les Européens et les Américains gravissent ensemble la dure pente des affaires humaines et spirituelles, plus ils s'élèvent dans l'échelle des valeurs, plus l'unité se rétablit et s'affirme, plus l'essentiel est retrouvé et confirmé en commun. *L'affluent society* prête à la facilité, au piétinement au niveau élémentaire. Dans les grandes crises de notre siècle, quand l'essentiel entre en jeu, l'unité fondatrice des deux formes de la culture occidentale retrouve ses vertus , de grands sacrifices l'ont, récemment encore, montré.

Il ne faut pas craindre des différences culturelles : elles rendent les dialogues et la collaboration féconds, aussi longtemps qu'on se donne pour fin, non pas un conformisme abêtissant, mais une compréhension fondée sur des différences justifiées. C'est de l'avenir de notre culture occidentale, à la fois commune et dédoublée, qu'il s'agit.

CHAPITRE 7

Commerce électronique, marketing et liberté

Philippe LEMOINE

Les interrogations sur le commerce électronique portent sur l'évolution du triptyque production de masse / communication de masse / consommation de masse. Durant un demi-siècle, ces trois forces ont tiré le devenir des économies occidentales. Internet et le commerce électronique dessinent un avenir nouveau où la technologie semble devoir faire table rase de tout cela.

Dans ce triptyque, les trois volets ne sont toutefois pas de même nature. La *production de masse* renvoie à un mode d'organisation industrielle, perfectible aujourd'hui par la mise en œuvre de nouvelles méthodes de gestion de la production : production flexible, flux tendu, réponse rapide, informatisation de la *supply chain*. La *communication de masse* est symbolisée par des médias, et d'abord par la télévision dont l'équilibre économique va être bouleversé par une évolution technologique qui fait chuter les coûts de production et plus encore de transport des images, ouvrant la voie à une hyperfragmentation des programmes et à une interactivité au niveau des personnes. La *consommation de masse,* elle, est d'une autre nature: elle renvoie à des comportements humains et sociaux, dont l'évolution du commerce est un reflet.

Quel est précisément le devenir de cette consommation de masse ? Le commerce entend désormais « gérer la relation client ». Il mobilise le potentiel de la technologie à cette fin. « Le chaland anonyme cède la place au client identifié », avions-nous écrit, il y a déjà sept ans[1]. Les uns saluent cette évolution comme bénéfique, en s'enivrant du vaste terrain qui s'ouvre à l'action et qui va permettre de créer de la différence par rapport au modèle ancien des « usines à vendre » et de la grande distribution. D'autres s'inquiètent des risques de dérive auxquels pourrait conduire un espionnage de la vie quotidienne dans ses moindres détails: marques préférées , quantités consommées ; date, heure, lieu d'achats ; modes de paiement; cigale ou fourmi ; normal ou pathologique; cru ou cuit; végétarien, régime ou casher ; cuir ou flanelle, etc. Le débat ne s'arrête pourtant pas là.

[1] Philippe Lemoine, *Le commerce dans la société informatisée,* Economica, 1993.

Trois facteurs viennent en effet complexifier l'analyse. Le premier est *l'extension de la sphère marchande* : on était hier client d'un monde de magasins et, d'une tout autre manière, on avait un compte sur une banque, on était assuré par une compagnie, on était abonné à un journal, on était usager du téléphone, on était membre d'un cercle, on était ami d'un musée, on était contribuable, patient, élève et, à temps perdu, citoyen. Tout cela semble fini. Vendeurs de biens ou de services, services privés ou publics, État même (pourquoi pas ?) : chacun ne s'adresse plus qu'à des clients. Le langage est devenu homogène, au moment même où la technologie parait pouvoir fournir des plates-formes transversales d'intermédiation. Et comme la logique marchande s'étend, la rationalité de l'échange s'impose à toutes ces occasions de recueillir et de traiter des informations. Faut-il s'inquiéter ou non de la recomposition possible de ce puzzle indéchiffrable qu'était hier le système de relations entre une personne et les institutions ?

Le second facteur à prendre en compte, *c'est l'éclatement des frontières et la mondialisation* que permet la technologie. Cette évolution complique la mise en œuvre d'une législation et d'un contrôle. Mais, à l'inverse, elle favorise une diversité d'initiatives qui perturbe l'idée d'une intégration croissante des logiques et des données. Aujourd'hui, avant la montée en puissance du commerce électronique qui est annoncée, avant même l'an 2000, on estime en effet que plus de 2 millions de sites marchands sont déjà ouverts. Ils sont tous accessibles à chacun d'entre nous, dès lors que l'on est connecté au réseau. Dans cet univers où le nombre des marchands immédiatement accessibles par chacun s'accroît à grande vitesse, comment imaginer que s'organise une mise en commun des connaissances, une mise à jour des informations, une mise à nu des individus ?

Les technologies mises en jeu sur Internet ne sont d'ailleurs pas principalement des technologies visant à permettre à des institutions de « tracer » des comportements pour mieux « cibler » des consommateurs. Les innovations les plus fortes se rattachent plutôt au champ des technologies permettant aux personnes de naviguer sur ce réseau mondial, de sélectionner des sites, de passer de l'un à l'autre, de comparer des informations piochées ici ou là. D'où le troisième facteur à prendre en compte et qui est *la nature profonde d'une technologie adaptée à une interactivité en univers complexe* : les langages de programmation utilisés, les mécanismes de liens hypertextes, les procédés d'agents intelligents permettant à une personne de « surfer », c'est-à-dire en fait de commander un déroulement d'écrans selon des logiques qui paraissent échapper à toute prédétermination. Les institutions ne peuvent plus enfermer les personnes dans des arborescences informatiques figées. Mais quelle liberté laisse-t-on à celui qui peut feuilleter à l'infini un livre sans limites et, plus encore, à qui l'on donne les moyens d'en désarticuler et d'en recombiner chaque phrase et chaque mot ?

Les problèmes d'organisation du nouvel espace marchand ne se résument pas à ceux d'un équilibre à trouver entre le *push* (la vision classique d'un jeu

dominé par des institutions qui proposent et qui sollicitent) et le Pull (le projet ou le mythe d'un système entièrement tiré par les personnes). Ils renvoient à la question des principes unificateurs de la société dans un contexte où la multifragmentation peut apparaître comme gérable sur tous les plans : niveaux de richesse, centres d'intérêts, composantes de la personnalité elle-même, puisque la navigation dans la complexité externe sollicite immanquablement le thème du voyage et des raccourcis dans l'exploration et la mise sous tension de la complexité intérieure de chacun. *Quid* de la connaissance ? Q*uid* des compétences ? Q*uid* de la religion ? *Quid* des pensées et des opinions ? Q*uid* de la mode et des courants ? Q*uid* de l'unité de la personne ?

Ce sont ainsi des interrogations complexes, difficiles, contradictoires, fondamentales, dérangeantes, chaudes déjà et parfois brutales, qui apparaissent dès que l'on creuse cette question des nouvelles technologies et du devenir de la consommation de masse. En fait, c'est toute la problématique « Informatique et libertés » qui remonte à la surface, alors qu'on la croyait enfouie, gelée, passablement froide. L'angle n'est toutefois plus le même. Les questions « Informatique et libertés » avaient été soulevées en Europe, dans les années soixante-dix, autour des risques de l'informatique administrative et du Léviathan. C'est que l'époque n'était pas la même non plus : l'informatique était encore une affaire de grandes organisations; elle paraissait liée à la poussée du seul modèle américain; l'Europe tardait à se confronter aux enjeux des droits de l'homme et du totalitarisme.

Aujourd'hui, les interrogations ne viennent plus seulement d'Europe mais également des États-Unis; donc d'un pays où il n'y a pas de loi généraliste sur « Informatique et libertés ». Ce qui est visé, ce n'est pas l'informatique des administrations, c'est l'informatique des marchands ; et c'est le commerce électronique qui est l'occasion d'un débat que nous ne connaissons pas encore vraiment en Europe. Interrogés dans des sondages, les internautes américains placent les questions de *privacy* comme le principal problème soulevé par le développement du commerce électronique. Plus étonnant encore: ils sont une majorité à demander une loi sur le modèle européen[2].

On assisterait donc à un double chassé-croisé. Les États-Unis semblent remplacer l'Europe comme foyer d'inquiétudes et d'interrogations. Les risques d'une technologie aux mains des marchands se substitueraient à ceux d'une technologie au service des États. Dans l'imaginaire collectif, la bascule est loin d'être neutre. A-t-on liquidé l'effort de mémoire sur le phénomène totalitaire qui était présent en creux dans la première vague des interrogations « Informatique et libertés » ? Sommes-nous en état de penser le monde futur en étant libres de toute réminiscence du passé ? Ou, au contraire, ne risquons-nous pas de mener une réflexion insidieusement alimentée par des images d'un autre temps, celle des marchands tirant secrètement les fils d'une société blonde et innocente ?

[2] Harris Poll, in *Business Week*, 16 mars 1998.

Je voudrais avancer ici sept axes de réflexion.

1. Les enjeux soulevés par le commerce électronique sont bien des enjeux de libertés, publiques et privées, et ne se résument pas à des questions de *privacy*

Aujourd'hui, on ne peut pas fréquenter un site élaboré du commerce électronique américain sans rencontrer une rubrique *privacy*. Les gestionnaires du site n'ignorent pas en effet qu'il faut répondre à une préoccupation. Et que répondent-ils ? Parfois, un avertissement technique est donné pour que l'internaute mette en œuvre telle ou telle procédure, afin d'éviter un enregistrement de données ou de bloquer la mise en place d'un fichier-espion, d'un *cookie*. Parfois, des engagements sont pris sur la non- commercialisation ou la non-réutilisation de tout ou partie des données collectées.

Plusieurs exemples ont illustré le fait que l'on ne pouvait pourtant pas accorder une confiance excessive à ce type de promesses et d'autorégulation. Tout va trop vite sur Internet et trop d'acteurs perdent encore trop d'argent. La tentation est donc grande de faire monnaie des données collectées. Même des sites affichant une philosophie communautariste et non marchande ont rompu le pacte moral qui les engageait et se sont alliés, avec leur stock d'informations et les restes de leur capital de confiance, à des sites commerciaux bien plus classiques.

Aussi le sentiment émerge-t-il que les enjeux soulevés par ce nouvel espace marchand qu'est Internet, vont bien au-delà d'une question d'accord contractuel entre une personne et un marchand quant au respect de la vie privée. Qui peut en effet nous protéger des faiblesses morales de notre interlocuteur ? Qui peut nous protéger des faiblesses techniques de ces systèmes, toujours violables, toujours perçables ? Qui peut nous protéger des pouvoirs de tous types, en période de guerre ou de troubles notamment, et qui pourraient exiger l'accès à tel ou tel secret ? Qui peut nous protéger surtout contre nous-mêmes, si nous résumons tout cela à une question de « vie privée » ?

En comparant le problème des données informatisées au problème de la photographie et du droit à l'image, l'idée peut venir que les données sur soimême seraient un bien personnel que l'on peut vendre ou échanger. Qu'est- ce qui peut empêcher alors l'apparition d'un vaste système de troc où les plus faibles et les plus démunis seront appâtés par des propositions fondées sur l'échange d'une gratuité clinquante contre une multitraçabilité discrète et rampante ? Aux États-Unis, le marketing utilise déjà l'ambiguïté du terme *free* pour qualifier toutes les propositions, depuis l'acquisition d'un micro-ordinateur jusqu'à un abonnement à Internet, qui mixent la gratuité et la mise en jeu de la liberté.

L'ambiguïté de la *privacy* apparaît particulièrement dans les systèmes les pl-us sophistiqués d'intermédiation où un opérateur-intermédiaire propose un confort accru de navigation sur Internet, grâce à l'auto-établissement, par une personne, de son propre profil. À la sortie de ces systèmes, un programme anonyme, un « agent intelligent », va circuler librement sur un site ou sur plusieurs sites du réseau. Mais le passage par cette « chambre d'anonymisation » soulève encore plus de problèmes, tant on est impressionné par la variété des informations qui sont alors collectées. Et systématiquement, cette étape est pourtant qualifiée de procédure de *privacy* !

Les enjeux débordent le cadre de ce paquet commode de la *privacy*. *Ils* rejoignent toutes les questions des libertés individuelles, des libertés d'aller et venir, celles qui sont à la base du commerce moderne. Ils rencontrent les enjeux de libertés publiques, ceux qui conditionnent le regard que nous portons sur la démocratie et sur une société ouverte.

2. Si l'enjeu ne se résume pas à la privacy, c'est d'abord parce que la consommation de masse ne s'analysait pas seulement comme un état d'anonymat, mais également comme un projet : celui d'une société pacifiée par un large accès au Bien et au Beau

Dans *Internet et après* ?, Dominique Wolton analyse avec bonheur comment le discours positif sur Internet s'appuie souvent sur une méconnaissance du monde des médias grand public traditionnels, qu'il tend même à caricaturer pour entretenir un sentiment de progrès[3]. Des débats techniques sur les nouveaux terminaux domestiques, par exemple, sont chargés d'émotivité, opposant le monde du PC à celui de la télévision. La télévision est alors présentée comme un instrument archaïque, unidirectionnel, antérieur à l'idée d'interactivité, sans que l'on fasse l'effort de restituer les valeurs et les projets autour desquels elle s'est développée.

Il en va de même avec le monde du commerce et de la consommation. Ce serait une vision biaisée de ne retenir que la question de l'anonymat comme ligne de partage entre la « grande distribution » et les voies nouvelles qu'esquisse le commerce électronique. La notion de consommation de masse est en effet marquée par une histoire chargée de valeurs et de projets.

Bien avant Henry Ford et l'idée que les ouvriers seraient les premiers consommateurs de leur propre production, la révolution industrielle avait favorisé des débats qualitatifs et exigeants sur la consommation. À la fin du XIX^{e} siècle, des controverses passionnées étaient apparues, en particulier dans les

[3] Dominique Wolton, *Internet et après ? Une théorie critique des nouveaux médias,* Flammarion, 1999.

pays scandinaves et germaniques. Dans les écoles d'architecture et dans les ligues d'industriels, l'idée s'était imposée que le *sens* de la production industrielle en série était de déboucher sur une baisse des prix et donc sur une accessibilité des produits, tout en permettant de répéter à l'identique un modèle et donc de pouvoir démocratiser le Beau.

Tout le mouvement du *design* moderne est né de cette interrogation. En Allemagne, le Bauhaus s'est nourri de la réflexion sur les liens entre rationalisation, fonctionnalisme et esthétique. Et c'est en Allemagne également qu'est- apparu, avant la seconde guerre mondiale, le thème de la consommation populaire. Dans un contexte menacé par la violence et par la haine, l'espoir était qu'un large accès au Bien et au Beau pourrait contribuer à pacifier la société. Les magasins populaires, les voitures populaires (Volkswagen), le théâtre populaire ont marqué cette époque.

Après la guerre, la joie de la paix et la joie de consommer à nouveau se sont conjuguées pour renouer avec ces thèmes. Mais le terrain avait changé. Le foyer central de l'économie et de la production était sans conteste les États-Unis, et nombre d'Européens impliqués dans l'esthétique industrielle se retrouvèrent en Amérique pour diffuser l'idée que la laideur ne fait pas vendre. Plutôt que de consommation populaire, il faut désormais parler de consommation de masse, car la problématique du *design* se confond alors avec la force montante de la publicité et des mass-média, d'une part, du commerce sur parking et du déploiement des libres-services, d'autre part[4].

Dès les années 1950, le règne de la consommation de masse est clairement affirmé, entretenu par l'idée rassurante que le Bien privé rejoint le Bien public et que, cahin-caha, la société chemine vers un avenir plus beau.

3. Bien avant que l'anonymat de la consommation ne soit levé, le marketing informatisé avait démantelé ce projet, en forgeant des « artefacts » (sociotypes, courants socioculturels) occupant le devant de la scène, au détriment des êtres humains

L'objet n'est pas ici de retracer une histoire des cinquante dernières années de la consommation. Il faudrait se référer à des mouvements sociaux divers, notam ment ceux des années 1960 où s'exprima la critique de l'« homme unidimensionnel » et de la « société de consommation ».

Le propos est d'illustrer comment la technologie a interagi avec le projet d'une consommation de masse, en soulignant que les thèmes de la fragmentation et de la diversification ont largement précédé le thème de la levée de l'anonymat.

[4] Philippe Lemoine, « L'objet postindustriel », *Autrement*, février 1982.

Jusqu'à la fin des années 1960, la technologie favorise les modèles intégrateurs et massifiants. Ce sont les caisses enregistreuses produites par NCR et promues dans le centre de démonstration de Dayton (Ohio) qui sont à l'origine du déploiement du libre-service. La modélisation économique sur ordinateur prolonge les efforts antérieurs d'établissement d'une comptabilité nationale et place la consommation au centre des « comptes de la puissance » d'une nation moderne[5]. Quant au marketing, il s'appuie avant tout sur des enquêtes d'opinion, souvent sous-tendues par une question sur l'acceptabilité d'une innovation technique ou sur l'état de progression d'un nouveau produit, selon un modèle de diffusion linéaire dans les différentes couches de la société.

La rupture provient d'une nouvelle génération d'outils statistiques : ceux de l'analyse multicritères, ou de l'analyse factorielle en composante principale. Il s'agit de procédés permettant de synthétiser des conclusions statistiques, tirées de l'analyse d'un tableau de données comprenant un grand nombre d'observations sur une population étudiée. En pratique, ayant interrogé *x* personnes, à qui l'on a posé *y* questions, l'analyse multicritères permettait de « positionner » ces *x* personnes dans l'espace à *y* dimensions de leurs critères de préférence ou de caractérisation.

Sur un plan technique, ce que l'ordinateur faisait, c'était de trouver le positionnement optimal d'un plan à deux dimensions venant couper cet espace théorique à *y* dimensions, tel qu'on minimise la perte d'informations lorsqu'on projette les différents points significatifs de l'espace multidimensionnel *y* sur l'espace plus pauvre à deux dimensions. Le résultat de ces analyses statistiques était ces fameuses « patatoïdes » qui ont envahi le discours marketing des années 1970-1980 et qui étaient en fait le produit d'une analyse multicritères où l'on avait projeté sur une feuille de papier à la fois des individus (les membres de la population étudiée) et des caractéristiques (les différentes rubriques du tableau de données).

Tout l'art du marketing à cette époque consistait à analyser de manière significative la proximité relative de ces individus et de ces caractéristiques. On cherchait alors le sens des coordonnées principales de la « carte » (nord / sud, est / ouest) et on établissait quatre, cinq ou six regroupements aux contours arrondis. Les conclusions de l'analyse reposaient sur le fait de dénommer ces « patatoïdes » et d'y voir des regroupements signifiants, permettant de caractériser des tempéraments (« cigales », « fourmis » ...), des courants socioculturels (« aventuriers », « utilitaristes », « terriens enracinés », « décalés » ...), des humeurs, des attitudes face aux propositions des appareils industriels, idéologiques ou commerciaux.

D'un point de vue théorique, il était *impossible* de passer de ces catégories d'analyse à des catégories d'action. L'informatique servait à déconstruire l'idée de

[5] François Fourquet, « Les comptes de la puissance : histoire politique de la Comptabilité nationale et du Plan », *Recherches,* 1980.

consommation de masse, l'idée de marchés intégrés, « seulement » découpés par les traditionnels clivages sociaux. Mais elle ne pouvait s'attaquer à la déconstruction du modèle central qu'en donnant à voir des « artefacts » statistiques, ne correspondant, terme à terme, à aucun individu en chair et en os. La précaution devait d'ailleurs être toujours prise de rappeler que personne n'est à 100% une « cigale », un « décalé » ou un « moderniste utilitariste ». On ciblait alors des types purs, non des individus.

4. Le thème du *one-to-one* est apparu lorsque la technologie a pu retrouver l'homme derrière les artefacts, en s'inspirant des outils nés de la segmentation comportementale, d'une part, des catalogues électroniques de l'armée, d'autre part

Le moment important dans l'apparition d'une nouvelle problématique « marketing », profondément distincte de celle de la consommation de masse, est le moment où la technologie se reconnecte à l'homme réel et non à un artefact statistique.

Or, ce qui est intéressant, c'est que cette reconnection ne s'opère pas par une sophistication plus poussée des analyses multicritères de données, mais par des outils beaucoup plus simples, employés de surcroît dans deux contextes très différents, voire contradictoires.

Le premier contexte est celui des *segmentations comportementales* telles qu'elles sont utilisées dans la vente par correspondance ou dans le crédit à la consommation, par exemple. Le point de départ est celui des grandes banques de données, comportant des millions de consommateurs. Sur chacun d'entre eux, on connaît des dizaines d'informations différentes. Mais le traitement que l'on va opérer pour agir à partir de cette base de données n'a rien à voir avec un *mapping* des éléments les plus fins du fichier. La question que l'on se pose est en effet de maîtriser un risque ou de maîtriser la rentabilité d'un investissement, dans une proposition commerciale que l'on entend faire à un client. Dans ce cadre, l'homme réel est ainsi l' « objet » d'une sollicitation déjà définie dont il s'agit de maîtriser la profitabilité.

Partant de là, l'expérience démontre que la connaissance des opinions, des caractéristiques sociographiques (CSP, âge ...), des variantes fines dans les achats effectués (marque, modèle ...) ne sert pratiquement à rien. Ce type de données qui est à la base de la plupart des artefacts utilisés dans les statistiques marketing est inopérant dans des programmes visant à établir une relation marketing directe avec un homme réel. Les données discriminantes sont des données strictement comportementales, reflétant les actes objectifs accomplis par les clients dans un passé récent.

Les professionnels du marketing direct s'en tiennent d'ailleurs généralement à deux critères très simples : la fréquence d'achat (nombre d'achats réalisés dans les douze derniers mois) et la récence (délai écoulé depuis le dernier achat). Dans la vente par correspondance, par exemple, les professionnels segmentent ainsi leurs fichiers en différentes catégories, en croisant ces deux critères principaux, de manière à séparer les très bons, les bons et les moins bons clients et à hiérarchiser l'importance des investissements en communication qui seront réalisés sur ces différents types de « cibles ».

Si l'on ajoute d'autres critères à ces éléments de base, il s'agira toujours de critères simples: le montant moyen d'achat, par exemple (le « panier »), ou le mode de contact utilisé par le client (lettre, téléphone, minitel, Internet). Toutes ces données ont fait la preuve qu'elles pouvaient être opératoires, mais cela va rarement au-delà. Le domaine du crédit à la consommation emploie certes des outils d'apparence plus sophistiquée, avec les modèles de *scoring*. Il existe ainsi des scores d'acceptation, permettant de déterminer le niveau de risques que l'on prend à accorder tel crédit à telle personne et, plus élaborés, des scores prédictifs de comportement, permettant de sélectionner le sous-ensemble d'une base de données qui réagira le mieux à une proposition commerciale. Mais ces outils restent des modèles pondérant de manière linéaire différents critères auxquels on a associé une valeur statistique, en fonction d'observations antérieures. Aucun de ces modèles ne repose sur une tentative de simulation du *comportement cognitif* du client, de la manière dont va se forger sa décision ou son désir.

Au total, l'homme réel, dans ce contexte de segmentation au sein des banques de données, est un individu pour lequel on dispose d'une probabilité statistique de réaction à une sollicitation définie en fonction de critères simples et objectifs, assez indépendants de la sophistication des données plus personnelles que l'on a pu collecter sur lui par ailleurs. Il en va tout à fait différemment dans le cadre d'une navigation sur un *catalogue électronique* et dans le contexte de ce que les Américains appellent, depuis près de dix ans, *electronic commerce*.

Le contexte dans lequel cette deuxième batterie d'outils est apparu n'a rien à voir avec le marketing direct, la VPC ou le crédit à la consommation. Il s'agit au départ d'outils mis au point par l'armée américaine pour faire face aux considérables réductions de crédits qui avaient été décidées après la chute de l'empire soviétique et du mur de Berlin.

Les gestionnaires militaires étaient alors à la recherche d'économies et il leur est apparu nécessaire de changer les méthodes de travail dans tout le cycle de conception et de mise au point des systèmes d'armes. Dans le domaine de l'électronique notamment, la réalisation de prototypes et d'outils sur mesure coûtait beaucoup trop cher. Avec leurs grandes séries de production, l'électronique et l'informatique grand public offraient souvent des fonctionnalités très proches, à

des coûts dix, cent ou mille fois moindres. Certes, il était souvent nécessaire de rajouter des coûts d'adaptation et d'intégration de systèmes, mais ce poste d'économies pouvait être capital.

Le département de la Défense américain s'est alors posé la question de savoir *comment* il allait convaincre les acheteurs et les responsables de projets technologiques de changer leurs méthodes de travail. Car cela ne revient pas au même d'être le client, même important, d'une industrie ou d'être le maître d'ouvrage imposant ses volontés et ses cahiers des charges à des fournisseurs sous-traitants. La difficulté était d'autant plus grande que tout le monde s'était habitué à une organisation de la recherche-développement où l'électronique militaire était censée « tirer » l'électronique civile. Il fallait d'un seul coup inverser le processus.

L'idée s'est alors imposée qu'il fallait d'abord que les responsables technologiques de l'armée connaissent l'offre et puissent interroger le marché. Dans un secteur d'innovation permanente, avec des produits aux fonctionnalités différenciées et complexes et des industriels toujours plus nombreux, le thème des catalogues électroniques interactifs s'est alors imposé comme une voie privilégiée pour accompagner ce virage des responsables vers un rôle d'acheteur intelligent et informé. Ce thème s'est rapidement conjugué avec celui d'Internet dont tout le monde connaît par ailleurs les origines militaires.

C'est ainsi que s'est constituée la deuxième source du marketing *one-to-one*. Contrairement à la segmentation comportementale, elle ne repose pas sur un support « figé » comme le papier, mais sur des supports malléables et interactifs. Elle ne provient pas d'instruments aidant au ciblage de l'offre mais à un rôle accru du client et de l'utilisateur. Il est d'ailleurs amusant de se remémorer que l'origine de tout le thème actuel du client-roi placé par la technologie au centre d'un système dont il gouverne les flux est né du personnage bien particulier qu'est l'acheteur militaire.

5. Le commerce de détail est invité à combiner et à utiliser massivement ces outils sur Internet, afin de créer une chalandise dans un contexte où les consommateurs-internautes peuvent être paralysés par la surabondance de l'information

L'environnement d'Internet incite en effet à développer un véritable marketing individualisé qui reposerait à *la fois* sur des outils de segmentation comportementale et sur des outils interactifs du type catalogue électronique. Comme dans le monde réel, il faut conquérir et fidéliser des clients et donc détecter des prospects, les solliciter, les faire venir, les faire acheter, puis les relancer par des propositions adaptées. Mais, contrairement au monde réel, il

n'est pas nécessaire de suivre ce cycle en proposant des offres « bouclées », même si elles ne sont pas uniformes et qu'elles ont été fragmentées en micromarchés. Sur Internet, il paraît possible de créer tout un relationnel avec le client, à partir d'offres personnalisées et qui vont être de plus en plus adaptées à ce client unique, au fur et à mesure qu'on va le connaître.

En termes techniques, cela signifie que la notion même d'un site organisé par un commerçant va s'effacer derrière l'idée d'un site recomposé autour de la démarche d'un client. L'entrée en matière, la *home page,* ne se fera pas sur les mêmes thèmes ou sur les mêmes produits, d'un client à un autre et d'une fois sur l'autre. La navigation ne sera pas non plus la même dès que l'on pénètre dans le « magasin virtuel ». Tout cela n'est possible qu'en accumulant un très grand nombre d'observations comportementales: pas seulement sur la récence, la fréquence ou le montant des achats, mais sur les trajectoires de navigation, sur l'habileté qu'elles dénotent, sur la dextérité dans l'utilisation d'Internet, sur la sophistication du terminal utilisé par le client, sur la manière dont il le domine, sur le temps qu'il met à effectuer des choix, sur le caractère plus ou moins décidé qu'il traduit , sur le contenu même des choix.

Toutes ces observations doivent être stockées dans des entrepôts de données *(datamart).* Grâce à des programmes sophistiqués en temps réel, ces observations sont censées pouvoir gouverner une réorganisation et une recombinaison de la structure des catalogues électroniques. Alimenté par des outils mathématiques et statistiques encore plus élaborés que ceux de l'analyse factorielle en composante principale, le *datamining* est ce vaste champ de recherche et d'application qui entend fusionner les deux univers disjoints de la segmentation comportementale et de l'organisation de l'offre commerciale.

Mais est-ce un mythe ou est-ce une technologie réellement opérationnalisable ? Le débat n'est pas vraiment tranché dans sa dimension scientifique et épistémologique. Sur un plan professionnel, les commerçants sont enclins au scepticisme et à la réserve. Les exemples souvent cités, à partir de l'expérience de Wal-Mart, d'une corrélation entre l'achat des couches pour enfants et l'achat de la bière, paraissent anecdotiques. Deux facteurs contribuent toutefois à donner corps à ce projet d'un marketing *one-to-one* global et hypertechnologisé.

Le premier facteur ne tient pas au commerce lui-même, mais à ses auxiliaires. Autant les commerçants se montrent en effet spontanément sceptiques sur une trop forte programmation de la relation marketing, autant il n'en va pas de même d'autres professions qui concourent à la structuration du nouvel univers de l'échange. Il en va ainsi des banquiers, tout d'abord, qui se sentent parfois menacés par la montée des technologies d'information et dont certains voient dans le commerce électronique une occasion de valoriser la connaissance poussée qu'ils ont de « leurs » clients. Aussi les propositions émanant du monde bancaire en matière de sécurisation des moyens de paiement

sont-elles souvent influencées par l'idée de renforcer la traçabilité et donc d'accroître encore la position de force relative de la banque dans ses relations avec ses partenaires commerçants. À la limite, « l'idéal » serait une situation où le banquier virtuel loue un de « ses » clients au commerçant virtuel et où il le loue cher, car il le loue avec un mode d'emploi.

Le monde de la publicité intervient également fortement dans la mise en œuvre de ces nouvelles technologies marketing. Comme tous les opérateurs sont prêts à acheter de l'audience sur Internet et à acheter une audience « qualifiée », les publicitaires sont incités à investir dans toutes les technologies de *tracking*. Les agences comme Double Click, rémunérées au « contact utile », sont dans l'obligation de connaître finement la population des internautes pour envoyer à chacun le bandeau publicitaire adapté et sur lequel il aura le plus de chances de cliquer.

Tous les groupes issus de l'informatique ou des télécommunications qui ont eu l'idée d'ouvrir des « galeries marchandes » ou des « centres commerciaux électroniques » sur le Net sont dans une problématique proche. Tels les gestionnaires du monde réel qui ouvraient des centres commerciaux en plein champ, ils prennent le risque de créer le trafic. Ils attirent les commerçants en leur demandant de verser un « loyer » minimal, sans vraie prise de risques, mais en consentant un pourcentage sur leurs ventes. Au centre commercial de rémunérer son risque, en créant du trafic ! Et comme ces acteurs viennent du monde de la technologie, il leur semble naturel d'utiliser une technologie avancée pour créer ce trafic.

L'autre grand facteur qui incite le commerce à aller dans le sens de ce marketing *one-to-one on line,* c'est le comportement des consommateurs eux-mêmes. La surabondance de l'information, la surabondance des sites, la surabondance des choix donnent l'impression que les gens sont un peu perdus. Des progrès considérables ont certes été réalisés pour faciliter l'ergonomie d'Internet, pour lui ôter le caractère rébarbatif d'un langage technique, inadapté au grand public. Mais la facilité même d'Internet génère parfois une sorte de crainte et de paralysie. On peut certes « surfer » sur le Net, mais où nous entraînera cette glissade ? En cliquant sur les mots soulignés, on ouvre des portes latérales qui entraînent, par la grâce de l'hypertexte, d'un univers à un autre. Ne sommes-nous pas plongés ainsi dans un labyrinthe dont on ne pourra pas ressortir? L'idée de la « toile d'araignée » qui est à l'origine du nom même de l'Intemet moderne (le « Web ») nous reste perceptible.

D'où l'importance qui s'attache à la question des « métaphores », des cadres mentaux qui peuvent être proposés aux particuliers de manière à ce qu'ils se sentent rassurés, disposant de points de repère, plongés dans un univers lisible. La difficulté, c'est de conjuguer des éléments, de telle sorte que les personnes se sentent à la fois libres et guidées. Et l'expérience a montré que nombre de métaphores ne « fonctionnaient » pas. Il en va ainsi, par exemple, de toutes les

tentatives qui ont été faites pour que le commerce virtuel offre un cadre ressemblant au commerce réel : linéaires de supermarché, Mall de centre commercial, boutiques sur une place de village. Toutes ces images ont été essayées et toutes ont échoué !

Le milieu des graphistes,, des ergonomes et des différents spécialistes du commerce électronique commençait à douter, lorsqu'une bonne nouvelle a été annoncée : la « personnalisation », cela marche ! Des tests avaient été réalisés pour comparer la fréquentation d'un site par les clients avec qui cette relation *one-to-one* avait été construite et par d'autres clients, au départ semblables mais à la personnalité de qui le site ne s'était pas adapté. Les écarts entre les deux populations s'avéraient très significatifs. Dans le domaine des livres, par exemple, Amazon.com a fait le choix de ne pas recourir seulement aux atouts de sa formule initiale : hyperchoix, prix promotionnels, accès à des critiques de livres, à des débats et à des commentaires. Désormais, lorsqu'on a déjà commandé chez Amazon, on est accueilli par une proposition sur la *home page* adaptée à ses centres d'intérêt et l'on reçoit chez soi des e-mails personnalisés de relance.

Un ingrédient important du commerce électronique parait ainsi avoir été trouvé. La question qui se pose, c'est alors de savoir pourquoi cela marche. Dans l'univers complexe d'Internet, *la métaphore la plus pertinente, ce serait soi-même.* Ce serait le reflet de ses propres traces qui procurerait la meilleure lisibilité. Pourquoi ? Narcissisme éternel ou question nouvelle à relier à l'interactivité ?

6. La question des métaphores et de leur efficacité amène à réinterroger le mythe de *Big Brother* avant qu'il ne s'impose comme horizon indépassable de la société d'information

Dans le cadre d'une interrogation prospective sur les libertés et sur l'avenir de la société informatisée, il est fondamental de constater que ce qui est au cœur de l'efficacité de ces nouvelles relations *one-to-one,* c'est l'adhésion des personnes elles-mêmes. Si les éléments des technologies et du savoir-faire qui composent cette forme de marketing parviennent à s'intégrer, ce n'est pas en raison d'un savoir scientifique ou professionnel. Le facteur décisif qui opère cette intégration, c'est le miroitement d'un mythe dont l'emprise est réelle sur l'esprit humain.

Au moment où ils formaient l'expression de « marketing *one-to-one* », Martha Rogers et Don Peppers[6] percevaient la nécessité de cette adhésion. Mais ils l'approchaient en termes quasi contractuels, comme un accord à trouver entre deux types d'intérêts. Le problème était de créer les conditions d'un marketing

[6] Martha Rogers, Don Peppers, *Le « one-to-one ». Valorisez votre capital-client,* Éditions d'Organisation, 1998.

« consensuel », point d'équilibre entre le besoin d'intimité des particuliers et le besoin de savoir des institutions. Jusqu'à un certain point, les personnes seraient d'accord pour se donner à connaître, si elles en perçoivent la contrepartie. Audelà de ce point, la contrepartie serait trop onéreuse pour qu'une entreprise en tire une ressource rentabilisable.

Pour un Européen, cette vision d'un *échange* possible entre l'intimité et le marché garde un aspect cynique et déroutant. Il y a tout juste un siècle, Paul Claudel avait ressenti le même choc au contact de la société américaine. Dans *L'Échange,* il s'interrogeait sur le rôle d'équivalent universel de l'argent[7]. Grâce à l'argent, un milliardaire parvenait à corrompre un jeune couple, sans que rien ne puisse résister: ni la jeunesse, ni la beauté, ni l'innocence, ni l'amour. Est-ce la même force d'échange universel qui parcourt les veines du réseau Internet ?

Oui et non. Les protocoles hypertextes permettent une imbrication poussée des logiques marchandes et non marchandes, selon des schémas inédits qui renforcent encore l'interrogation de Claudel. Mais ce qui est nouveau, c'est la condition de ce méta-échange ; de cette interopérabilité généralisée, de cette équivalence entre les contraires, c'est l'attrait que chacun éprouve pour son « double informationnel » dans le cadre d'un nouveau rapport à l'Autorité.

La question des libertés mettait en scène, traditionnellement, deux volontés distantes et inégales : celle du sujet et celle de son maître. Norbert Wiener avait annoncé que la cybernétique allait complexifier cette problématique et qu'il ne suffirait pas d'automatiser les travaux d'esclave pour faire disparaître le principe de l'esclavage[8]. De fait, dans l'univers du virtuel et de l'échange électronique généralisé, la liberté se déploie ou se comprime dans des distances apparemment miniaturisées mais étonnamment puissantes : l'intervalle entre soi et son double; celui entre soi, son double et cet être mi-semblable mi-différent qu'est son frère.

Car là où le commerce électronique représente une étape fondamentale pour ceux qui se préoccupent de libertés, c'est qu'il oblige à se poser la question de la métaphore centrale: Pourquoi l'expression qui s'est imposée, depuis des décennies et sur le globe entier, est-elle celle de *Big Brother* ? L'origine est le talent de George Orwell, bien entendu[9]. Mais pourquoi *Big Brother*, précisément ? Pourquoi pas *Big Father? ou Big Mother?*

Ce qui intrigue, c'est que l'Autorité soit représentée par une figure fraternelle. La société postaristocratique s'était construite sur l'abandon de toutes distinctions ou prérogatives selon le rang dans la fratrie : cadets et puînés avaient les mêmes droits que les aînés. La République avait placé la fraternité à son frontispice, comme valeur complémentaire des valeurs d'égalité et de liberté.

[7] Paul Claudel, *L'Échange*, Gallimard, 1977.

[8] Norbert Wiener, *Cybernétique et société,* Union générale d'éditions, 1962.

[9] George Orwell, *1984*, Gallimard, 1950.

Quelle société nouvelle, quel ordre nouveau émergent derrière ce nouveau statut de « grand frère » ?

L'étonnement est d'autant plus grand que cette nouvelle autorité ne s'est jamais définie par un pouvoir de coercition ou de répression; *Big Brother is watching you*, dit Orwell. Il vous surveille. Et alors ? Des parents définissent des règles, éduquent, punissent si l'on s'en éloigne. Un frère, lui, ne détient pas une autorité symbolique: il peut certes « moucharder » et devenir un auxiliaire de la justice parentale ; mais un grand frère est d'abord un interlocuteur, un modèle d'identité alternatif par rapport auquel on se situe dans des rapports de complicité, de bagarre, d'association. En simplifiant et en raccourcissant, on peut dire que le Père et la Mère sont des figures de la Loi et, donc, de l'État. Alors qu'un frère est une figure du contrat et du conflit, donc de la société civile. Où nous emmène alors *Big Brother*?

Big Brother sait tout, voit tout. On pourrait soutenir que *Big Brother* n'est finalement qu'un adulte, quelqu'un qui sait. Et en quoi le fait qu'il sache maintiendrait les autres dans une dépendance ? Que chacun cesse d'être dupe et devienne *Big Brother* à son tour ! La crainte de l'infantilisation généralisée serait un fantasme. Internet et l'informatique de grande diffusion pourraient permettre l'émergence d'une société de grands hommes, de *Big Brothers* généralisés !

Cette façon de raisonner est pourtant trop simple, car elle néglige le problème majeur de toute vie en société: celui du rapport à l'innocence. Un adulte dans une société libre, c'est quelqu'un qui a su accéder au Savoir, sans briser les conditions de l'innocence. Car il n'est pas besoin de pactiser avec le Diable : on peut savoir et rester innocent. L'homme n'est pas le Dr Faust. Mais de quelle innocence parle-t-on ?

Sur Internet, l'homme ou la femme veulent parfois avoir plusieurs identités ou se masquer derrière un pseudonyme. Ils se plaisent à confronter les rôles qu'ils jouent dans le monde réel et les traces qu'ils entretiennent dans le monde virtuel. Les institutions se plient à ces règles, parfois même avec humour. L'agent intelligent tridimensionnel *my model* s'adresse en ces termes à son auteur.: «.Bonjour, je suis ton double. Je te ressemblerai en fonction de ce que tu m'expliqueras de toimême, autant que tu le souhaiteras. Mais si tu me mens, je te mentirai aussi ! »[10]

Par nature, Hermès / Mercure, dieu du commerce, dieu de la communication, dieu des voleurs, s'adapte avec aisance à ces ambiguïtés : chacun peut être double dans le *one-to-one*. Là où tout change de nature, c'est au moment où l'on quitte le face-à-face, le masque-à-masque, pour admettre la présence d'un tiers, fusse-t-elle celle d'un frère. C'est là que s'impose la figure de *Big Brother*. Et les candidats ne manquent pas à vouloir tenir ce rôle. Combien d'acteurs veulent être

[10] Entretien avec Louise Guay, présidente de PTM (Public Technologies Multimedia); www.ptm.ca.

« tiers certificateurs », « tiers authentificateurs », « tiers de confiance » dans le monde Internet. Avec ces relations triangulaires, est-on encore dans le jeu ? Ou ne rentre-t-on pas dans l'invention de nouvelles formes de contrôle social ?

7. En s'appuyant sur le droit et sur la philosophie, l'Europe doit jouer un rôle indispensable dans la clarification de notre avenir, en commençant par séparer individualisation et personnalisation

Il n'est pas dans notre propos d'aller ici au bout d'une interrogation sur les relations entre l'échange, le commerce, l'autorité et les rapports triangulaires. Durant plus de trente siècles, notre société s'est développée à l'ombre du mythe d'Œdipe, La question que l'on peut se poser, au moment où chacun se plaît à consacrer la montée des valeurs féminines dans notre société, c'est de savoir si les technologies d'information et Internet ne contribuent pas à nous faire percevoir de *plus vastes changements encore,* dont *Big Brother* serait un signe avancé.

Une manière d'illustrer cette interrogation est de se référer à l'analyse que Claude Lévi-Strauss fait du mythe d'Œdipe[11]. Selon lui, la scène se joue en effet deux fois. Avant de franchir la distance qui aurait dû le séparer de sa mère, Œdipe franchit en effet la distance que chacun a respecté jusqu'alors, face à la connaissance. Interrogé par le Sphynx sur le chemin de Delphes, Œdipe se voit poser la célèbre énigme sur l'animal qui marche à quatre pattes le matin, à deux pattes à midi et à trois pattes le soir. Comme chacun le sait, il va répondre et pourra poursuivre son chemin, vers sa perte.

Ce qui doit étonner, note Lévi-Strauss, ce n'est pourtant pas qu'Œdipe réponde: l'homme. C'est que, jusqu'à lui, chacun ait préféré se faire dévorer plutôt que de déchiffrer cette énigme enfantine. N'est-ce pas le signe qu'il faut se garder de franchir une distance, celle qui a trait à la connaissance totale de l'homme ? Franchir cette distance, ce serait déjà violer la prohibition de l'inceste.

La société de l'information, l'économie de la connaissance ne peuvent pas s'inscrire dans ce mythe. Il faut pouvoir tout voir, tout savoir. « Il faut imaginer Sisyphe heureux », a pu écrire Albert Camus[12]. Peut-être. Mais chacun de nous peut observer un mythe en train de naître : Œdipe heureux. Car qui est donc *Big Brother,* si ce n'est Œdipe heureux ?

Par la philosophie et par le droit, l'Europe doit se donner les moyens d'aider le monde à traverser cette passe sans sombrer dans l'anomie et la perversité. Les technologies d'information progressent. L'économie se redéfinit. La démocratie est

[11] Claude Lévi-Strauss, cité dans Marc-Alain Ouaknin, *Les Dix Commandements,* Le Seuil, 1999.

[12] Albert Camus, *Le mythe de Sisyphe,* Gallimard, 1970

à la recherche de nouvelles références. La place des femmes et des hommes change dans la société. Nul ne peut encore, cependant, relier ces différents plans les uns aux autres.

Avec Internet, nous entrons dans un nouvel âge de l'échange. L'intermédiation prend un nouveau sens, et tout indique qu'il faut se méfier des risques juridiques, culturels et mentaux de certaines relations de triangulation ; rien n'est encore écrit sur l'avenir de la consommation de masse.

Sur le plan collectif, les enjeux soulevés sont graves et importants. Tout indique qu'il faut garder une dimension de « jeu » et se méfier de l'intrusion des logiques institutionnelles lourdes. Le nouvel univers de l'échange est complexe. Il est traversé par des mythes et porté par un principe de plaisir. Il serait déraisonnable de faire confiance à quelque tiers que ce soit, à quelque institution que ce soit, pour déterminer sa place par le seul jeu de l'ascèse et de l'autorégulation.

Pour des raisons symboliques, tout autant que pratiques, l'Europe doit affirmer avec force ce qu'elle a pressenti depuis plus de vingt ans : dans ces domaines, il faut faire une place à la loi.

CHAPITRE 8

Libre circulation des données et protection de la vie privée dans l'espace européen

François RIGAUX

Introduction (*)

Le droit, comme l'informatique, se construit selon un rythme binaire. Entre deux réponses à une question, l'une évince l'autre selon la logique du tiers exclu: l'accusé est coupable ou innocent, un être humain est un homme ou une femme, il est marié ou célibataire, un contrat est valable ou nul. Certaines réalités humaines résistent aux procédés de taxinomie binaire: il y a du féminin en tout homme et du masculin en toute femme. L'orientation sexuelle n'est pas non plus aussi tranchée qu'il pourrait paraître selon la division en hétérosexuels et homosexuels. On pourrait multiplier les exemples.

La nécessité de tenir en équilibre deux intérêts divergents, sans qu'aucun ne puisse, en principe, être sacrifié à l'autre, apparaît dans l'intitulé de la directive 95/46/CE du Parlement et Conseil des Communautés européennes du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[1]. La même paire apparaît dans l'intitulé de la présente contribution aux *Mélanges en l'honneur d'Ulrich Drobnig*. Ce n'est pas une division binaire qui les oppose. Il s'agit d'intérêts divergents sans doute mais que les auteurs de la norme prétendent concilier. L'un des objets de la présente étude sera de vérifier les limites d'un tel accomodement. L'« espace européen » auquel il est fait référence dans le même intitulé vise les deux principaux domaines scientifiques dans lesquels le Pr Drobnig s'est distingué : le droit international privé et la méthode comparative. Celle-ci a, en effet, été mise en œuvre pour l'harmonisation du droit à l'intérieur de la Communauté européenne, mais l'unification du droit n'a pas été à ce point complète qu'elle ait éliminé tout problème de conflit de lois.

À l'instar des instruments internationaux et des lois nationales qui l'ont précédée, la directive européenne prévoit l'institution d'autorités administratives indépendantes auxquelles le législateur étatique est invité à confier une mission de contrôle sur les banques de données à caractère personnel. Ainsi, la protection de droits individuels qui relèvent au premier chef de la sphère privée est assurée par des mécanismes de droit publie, jetant, une fois de plus, le discrédit sur la division dogmatique entre le droit privé et le droit public.

La suite de cette étude aura pour objet les problèmes suivants:

I/ Les divergences terminologiques

II/ La discordance d'objectifs fondamentaux

---

* *Ce texte ne donne pas toutes les notes de référence. Se reporter à l'article initialement publié dans* Festschrift für Ulrich Drobnig, zum siebzigsten Geburstag, *publié ici avec l'autorisation de l'auteur et du Max Plank Institut für ausländisches und IPR, Hambourg. Le secrétariat du groupe « Société d'information et vie privée », à l'Académie, tient le texte intégral à la disposition des lecteurs*

[1] JOCE, n° L. 281/31 du 23 novembre 1995.

III/ Le recours a des concepts indéterminés et le renvoi à la pondération d'intérêts concurrents;
IV/ L'immersion d'une nouvelle technologie dans des systèmes conceptuels préexistants;
V/ Les conflits de normes et leur pacification;
VI/ La détermination du domaine spatial du nouveau droit de l'informatique.

I/ LES INSTITUTIONS ET LES MOTS POUR LE DIRE

Un premier paradoxe est que les autorités de contrôle déjà existantes dans la plupart des pays européens exercent une activité qui est à peu près la même partout et a des visées identiques, alors que leurs fonctions ne sont pas désignées par les mêmes mots. Pareille divergence terminologique n'est sans doute pas sans portée. On peut y distinguer au moins trois orientations.

Ou bien le nom de l'autorité de contrôle désigne clairement l'objet et l'étendue de ses compétences : la protection de la personne à l'égard du traitement de données à caractère personnel. L'article 30 de la loi italienne n° 675 du 31 décembre 1996, l'une des plus récentes en la matière, est un exemple de cette première famille de dénomination : Garante *per la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*[2].

L'article 6 de la loi française du 6 janvier 1978 fait aussi, mais moins clairement sans doute, apparaître que le législateur a institué un organe nouveau chargé de la protection des libertés individuelles dans le domaine de l'informatique : *Commission nationale de l'informatique et des libertés*[3].

Ou bien la fonction est énoncée en termes plus généraux que ne l'implique la législation qui l'a instituée. Tel est le cas, notamment, pour l'article 22 de la loi belge du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, qui institue une « Commission de la protection de la vie privée » dont les compétences sont déterminées par les articles 29 à 31 de la loi sans qu'elles excèdent le secteur de cette protection, délimité en conformité avec l'intitulé de la loi[4]. Toutefois, le législateur a ultérieurement confié à la commission une compétence consultative en d'autres domaines de la vie privée[5]

Une troisième famille d'instruments législatifs désigne l'organe de contrôle par l'objet matériel de ses compétences, sans référence expresse à la volonté de protection des personnes. Le modèle en est procuré par les commissions de protection des données *(Datenschutzkommission)* des lois allemandes[6] ou par la *Registratiekamer* qu'a instituée l'article 37 de la loi néerlandaise du 28 décembre

---

[2] Pareille désignation du « garant » reprend l'intitulé de la loi *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, Gazzetta Ufficiale,* I, n. 3, 8 janvier 1997.

[3] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique et aux libertés, *Journal officiel de la République française,* 7 janvier 1978, p. 227.

[4] *Le Moniteur belge,* 18 mars 1993. En outre, avant le 8 décembre 1992, divers instruments de nature législative avaient déjà réglé la matière dans des secteurs particuliers. Voir, sur ce point : F. Rigaux, « La protection des banques de données et le respect de la vie privée », *Revue de droit de l'ULB,* 1994, n°, 3, 51-71.

[5] Loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées *(Le Moniteur belge,* 24 janvier 1995), art. 14.

[6] Selon le § 17 de la Bundesdatenschutzgesetz du 27 janvier 1977, *BGBI I,* S. 201 : « Es ist ein Bundesbeauftragter für den Datenschutz zu bestellen. » La loi de 1977 a été modifiée par la Gesetz zut Fortentwicklung der Datenverarbeitung und des Datenschutzes du 20 décembre 1990 *(BGBl*I, 2954), entrée en vigueur le l[er] Juin 1991.

1988[7]. Non moins que les précédentes, ces lois visent à la protection des personnes dont les données sont traitées par un procédé informatique, mais il reste que l'expression *Datenschutz* n'est pas dépourvue d'équivoque, Les données sont une marchandise dont la protection ne rejoint pas nécessairement la protection des personnes qui devraient en principe maîtriser elles-mêmes leurs propres données[8]. En outre, alors qu'à l'origine seuls les traitements automatisés étaient soumis à des règles spécifiques[9], le besoin est ensuite apparu d'étendre la protection aux fichiers manuels et aux « dossiers structurés »[10].

II/ PROTECTION DES INDIVIDUS ET LIBRE CIRCULATION DES DONNÉES

Les politiques législatives nationales tendent à la protection de la population de l'État à l'égard des traitements (automatisés ou non) de données à caractère personnel[11]. La transnationalisation et la délocalisation de l'outil informatique, la facilité avec laquelle les données passent les frontières ont très tôt fait apparaître la nécessité de soumettre les États à des normes communes. Deux organisations internationales, l'OCDE et le Conseil de l'Europe, ont, il y a quelque vingt ans, élaboré des textes qui convergent pour l'essentiel[12], en dépit des approches différentes qui y furent respectivement suivies.

Le Conseil de l'OCDE a adopté le 23 septembre 1980 une Recommandation concernant les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel. Cette recommandation a été publiée le 1er octobre 1980, précédée d'une préface et suivie d'un exposé des motifs qui en éclaire la portée[13]. Les lignes directrices *(guidelines)* sont annexées à la Recommandation.

---

7 « Wet van 28 december 1988, houdende regels ter bescherming van de persoonlijke levenssfeer in verband met persoonsregistratie (Wet persoonsregistratie) », *Staatsblad van het Koningrijk der Nederlanden*, 1988, rit. 665. L'article 37, alinéa 2 de là loi définit les compétences de la « chambre d'enregistrement » : « De Kamer ziet toe op de werking van persoonsregistraties overeenkomstig het bij en krachtens deze wet bepaalde en in het belang van de bescherming van de persoonfijke levenssfeer in het algemeen. »

8 Le « droit à la maîtrise des données personnelles » (Recht *auf « informationelle Selbstbestimmung »)* a été tenu pour un droit constitutionnellement garanti (BV*erf*G, 15 décembre 1983, *BVerfGE*, 65, 1, 43).

9 Tel était, par exemple, l'objet limité de la Convention du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Mais l'article 3, 3, *c* de la Convention permettait aux États d'en étendre l'application aux traitements non automatisés. Plusieurs dispositions de la loi belge du 8 décembre 1992 s'appliquent aux fichiers manuels.

10 Voir en ce sens le considérant (27) de la directive 95/46/CE du Parlement et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données *(JOCE,* n°, L. 281/31 du 23 novembre 1995). L'article 3, 1 de la directive en étend l'application au « traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier ». À la lumière du considérant précité, il faut inclure les dossiers structurés parmi les fichiers. La distinction élusive entre un dossier ou un ensemble de dossiers et un fichier a fait l'objet d'observations du Conseil d'État et de la Commission de la vie privée au cours des travaux préparatoires de la loi du 8 décembre 1992 (voir F. Rigaux, *op. cit.*, n. 4, n° 8).

11 Tant dans le texte de la Convention du 28 janvier 1981 (note 9) que dans celui de la directive du 24 octobre 1995 (note 10), l'expression « données à caractère personnel » désigne « toute information concernant une personne physique identifiée ou identifiable ». La même notion est exprimée dans le texte anglais par « p*ersonal data* », qui ne peut dès lors être traduit par « données personnelles ». La terminologie italienne est, sur ce point, plus proche de l'anglaise que de la française.

12 La convergence n'est pas fortuite. A l'exception de Chypre et de Malte, tous les États membres du Conseil de l'Europe (en 1980) étaient aussi membres de l'Organisation de coopération et de développement économique (OCDE), qui inclut en outre cinq États non européens, l'Australie, le Canada, les États- Unis, le Japon et la Nouvelle-Zélande.

13 *Publication de l'OCDE,* Paris, 1980, 42 p.

Datant du 28 janvier 1981, la Convention du Conseil de l'Europe (supra, n. 5, p. 27) est de nature plus contraignante, bien que les dispositions qu'elle contient ne soient pas directement applicables (art. 4, 1). Sur ce point, elle n'est pas sans analogie avec la directive communautaire déjà citée (*supra*, n. 6, p. 27).

Ce qui distingue le plus la Recommandation de l'OCDE de la Convention du Conseil de l'Europe est une question d'accent. Sans doute l'une comme l'autre s'efforcent-elles de « concilier des valeurs à la fois fondamentales et antagonistes, telles que le respect de la vie privée et la libre circulation de l'information », ainsi qu'il est écrit au début du préambule de la Recommandation et dans le dernier considérant de la Convention. En revanche, les autres motifs de chacun des deux préambules insistent sur une seule des deux « valeurs » jugées antagonistes : les deux premiers considérants du préambule de la Convention réaffirment la prééminence du respect des droits de l'homme et des libertés fondamentales, tandis que les trois derniers alinéas du préambule de la Recommandation insistent sur la contribution des flux transfrontières au développement économique et social[14].

Bien que la Communauté européenne soit au premier chef une organisation économique, la directive du 24 octobre 1995 s'efforce à une présentation plus équilibrée des deux objectifs qu'elle vise : « Respecter les libertés et droits fondamentaux [des] personnes, notamment la vie privée, et contribuer au progrès économique et social, au développement des échanges ainsi qu'au bien-être des individus. » [15]

Alors que l'hypothèse même d'une circulation transfrontières des données était plutôt: perçue avec inquiétude par les premières lois nationales de régulation, elle forme la substance même des instruments internationaux ou communautaires, l'harmonisation des normes protectrices sous la garantie du respect de certains principes fondamentaux étant la condition nécessaire, mais jugée suffisante, de la libre circulation des données. Le considérant (11) de la directive rappelle encore que ces principes se laissent déjà déduire de l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950. Cela signifie que la victime individuelle d'une violation du droit au respect de la vie privée peut adresser à la Commission européenne des droits de l'homme une requête dirigée contre l'État qui pourrait en être tenu responsable[16].

En dépit des formulations balancées s'efforçant de concilier des objectifs antagonistes, force est de constater que tous les instruments actuellement en vigueur, qu'ils soient nationaux, internationaux ou communautaires, sont traversés par le conflit de plusieurs libertés, la liberté de l'information, la liberté du commerce et des échanges, la liberté de la vie privée sous la forme spécifique de la maîtrise par chaque sujet des données relatives à sa personne, à son histoire, ses activités, ses

---

14 Pour une comparaison plus détaillée des deux instruments, voir, notamment: F. Rigaux, « La loi applicable à la protection des individus à l'égard du traitement automatisé des données à caractère personnel », *Rev. crit.* dip, 1980, 443-478, nos 13-17.

15 Préambule, considérant (2). Les considérants (3) à (l 1) maintiennent cette rédaction balancée avec, toutefois, une insistance répétée sur les exigences du « marché intérieur », lequel implique la libre circulation des données, selon le considérant (3).

16 Parmi les instruments internationaux, on signalera encore la Convention d'application de l'accord de Schengen du 14 juin 1986 entre les gouvernements des Etats de l'Union économique Benelux, de la République fédérale d'Allemagne et de la France, relatif à la suppression graduelle des contrôles aux frontières communes, signée à Schengen le 19 juin 1990. La Convention d'application est actuellement en vigueur entre les États qui l'ont conclue, auxquels se sont joints l'Autriche, l'Espagne, la Grèce, l'Italie et le Portugal. Le chapitre Il (art. 93 à 101) a pour objet l'exploitation et l'utilisation du Système d'information Schengen, tandis que le chapitre III veille à la protection des données à caractère personnel (art. 102 à 118). La fiabilité et la sécurité des données priment le droit au respect de la vie privée sans totalement l'évincer, Voir, notamment : Lucia Serena Rossi, « La protezione dei dati personali negli accordi di Schengen alla luce degli standardo fissati dal Consiglio d'Europa », in Da *Schengen* a *Maastricht*, ed. Bruno Nascimbene, Milano, Giuffrè, 1995, p. 173-201.

opinions, sa religion, sa vie familiale, ses maladies, les infractions dont il a été accusé ou convaincu. De nombreux articles de la directive communautaire portent la trace de l'indécision du législateur et révèlent l'impossibilité de régler la matière par des normes préétablies, sûres et contraignantes.

III/ LES CONCEPTS INDÉTERMINÉS ET LES RÈGLES CONDITIONNELLES

L'ambivalence d'objectifs plus contradictoires que complémentaires entraîne des hésitations dans la rédaction des textes et l'accumulation d'incertitudes qui vont bien au-delà du recours occasionnel à des concepts indéterminés *(unbestimmte Begriffe).* Plusieurs articles de la directive communautaire et davantage encore le préambule illustrent ces observations.

En dépit du projet ambitieux annoncé dans le considérant (11) de la directive, aux termes duquel « les principes [...] contenus dans la présente directive précisent et amplifient ceux qui sont contenus dans la Convention, du 28 janvier 1981, du Conseil de l'Europe... », la directive abonde en normes conditionnelles. Citons quelques exemples.

Contenant plusieurs « principes relatifs à la légitimation des traitements de données », l'article 7 prévoit une série de légitimations alternatives dont la dernière pourrait supplanter toutes les autres. En effet, à la lettre *f)* il est écrit que le traitement de données à caractère personnel peut être effectué si :

> il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er, § 1.

Le considérant (30) contient quelques indications sur la nature des activités qui pourraient justifier l'intérêt légitime requis, mais il reste incertain si le législateur étatique peut se borner à introduire dans son ordre interne une norme reproduisant la double indétermination contenue dans le texte communautaire reproduit ci-dessus : quelle est l'étendue des intérêts « légitimes » ainsi ajoutés aux justifications plus précises des lettres a à e du même article, et, surtout, en quoi la référence aux termes très généraux de la garantie procurée par l'article 1er, alinéa 1er, va-t-elle circonscrire l'équilibre à maintenir avec un intérêt tenu pour légitime. Il est douteux qu'aucun législateur soit en mesure de préciser la portée d'un texte aussi vague, qui se borne à poser un problème sans y apporter de solution. Il appartiendra sans doute aux autorités de contrôle, nationales et communautaire, le cas échéant aux cours et tribunaux et, en dernière analyse, à la Cour de justice, de se prononcer sur l'interprétation du texte à la lumière des litiges particuliers qui leur seront soumis[17].

L'article 7 *f)* est particulièrement significatif parce qu'il met en balance deux notions indéterminées: un intérêt qualifié de légitime (alors qu'on attendrait plutôt du législateur qu'il distinguât ce qui est légitime de ce qui ne l'est pas) et le seul principe du droit au respect de la vie privée. Mais d'autres articles de la directive recourent aussi à des concepts peu ou non déterminés, tels l'article 11, alinéa 2 (« l'information de la personne concernée se révèle impossible ou implique des

---

[17] Bien que la Cour, saisie d'une question préjudicielle d'interprétation du droit communautaire, soit sans compétence pour se prononcer sur l'application du texte à un litige particulier, elle ne laisse pas de prendre en considération les particularités du cas litigieux pour formuler sa propre interprétation. Comp. Ulrich Damman et Spiros Simitis, *EG-Datenschutzrichtlinie* (Baden-Baden, Nomos Verlagsgesellschaft, 1997), p. 152-153, avec une note de scepticisme quant à la possibilité d'atteindre à l'harmonie par cette méthode.

efforts disproportionnés ») ou l'article 13, alinéa 2 (« dans le cas où il n'existe manifestement aucun risque d'atteinte à la vie privée de la personne concernée »).

IV/ L'INSERTION DES PRINCIPES DE DROIT COMMUNAUTAIRE DANS LES SYSTÈMES CONCEPTUELS DE DROIT INTERNE

À l'instar des instruments internationaux d'harmonisation du droit interne, la directive utilise des concepts dont la résonance en chacun des ordres étatiques où ils seront mis en œuvre dépendra du sens qu'ils sont aptes à y recevoir. Le noyau de la plupart de ces concepts est certes commun à tous les États destinataires de la directive sans que les contenus en soient pour autant identiques. Les concepts de consentement et de responsabilité sont particulièrement significatifs à cet égard.

Modalités diverses du consentement

Affirmé par le Tribunal constitutionnel fédéral allemand (supra, n. 4, p. 27), le principe du « droit à l'autodétermination informationnelle » devrait entraîner que tout enregistrement de données fût subordonné au consentement de la personne identifiée ou identifiable à laquelle se réfèrent les informations recueillies. L'importance de la question est telle que l'article 2 h) de la directive contient une définition du consentement à laquelle on ne trouve guère de parallèle dans les Codes civils usuels :

> Aux fins de la présente directive, on entend par:
>
> *h)* « consentement de la personne concernée » : toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement[18].

Non seulement chacune des trois épithètes qui qualifient la manifestation de volonté — et le mot « volonté » lui-même — nécessiterait une définition, mais quelque circonstanciée qu'elle fût, la définition initiale n'a pas paru suffisante, et la lettre *a*) de l'article 7 y ajoute une quatrième épithète, également peu habituelle .en droit civil: que « la personne concernée a indubitablement donné son consentement ». L'adverbe signifie sans doute que le consentement doit obéir à une preuve particulièrement exigeante, mais on conçoit difficilement que la forme en laquelle l'exigence est formulée par la directive soit reproduite dans les mêmes ternies dans la législation nationale : Qu'est-ce qu'un consentement dont il serait permis de douter ?

À l'article 8, qui a pour objet le traitement des « données sensibles »[19], la notion de consentement apparaît accompagnée d'un autre qualificatif. La prohibition du

---

[18] Dans leur commentaire de l'article 2b), Damman et Simitis insistent à plusieurs reprises sur un passage du texte allemand de cette disposition qui n'a pas d'équivalent exact dans les textes français et anglais : « Einwillingung der Betroffenen » est définie : « Jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachbage erfolgt... » Dans les textes anglais et français, les mots

« für den konkreten Fall » ont été traduits par « spécifiques », *specific,* qui sont loin d'avoir la même portée, Comme la directive a été élaborée à l'époque de la présidence allemande de la Communauté, l'influence des juristes allemands sur sa rédaction a été, à tort ou à raison, avancée.

[19] Pour une analyse critique de cette notion, voir notamment Spiros Simitis, « "Sensitive Daten" — Zur Geschichte und Wirkung einer Fiktion », *Festschrift zum 65. Geburtstag von Mario M. Pedrazzini* (Verlag Stampfli und Cie AG, Berri, 1990), p. 469-493. Dans le commentaire récent de la directive cité à la note 1, p. 31, les auteurs critiquent assez sévèrement l'ensemble de l'article 8, « l'un des éléments les plus problématiques de la directive » (Damman/Simitis, p. 159). La notion de « données sensibles » est tenue pour « unidimensionnelle » et apparaît en conséquence comme trop englobante par certains aspects, insuffisante par d'autres (p. 160).

traitement des catégories de données énumérées à l'alinéa 1er est levée lorsque « la personne concernée a donné son consentement explicite à un tel traitement... »[20] . Le sens de l'épithète parait ici assez clair : il faut que le consentement ait eu pour objet explicite le traitement de l'une des données énumérées à l'alinéa 111. Mais l'emploi de ce terme invite à poursuivre la réflexion sur le sens du caractère indubitable du consentement dans l'article 7, *a)* : un consentement peut-il recevoir cette qualification tout en étant implicite ? La réponse affirmative paraît la plus vraisemblable, surtout si l'on compare ces deux textes à une autre disposition, elle aussi d'origine communautaire, l'article 3, alinéa 1er, de la Convention de Rome du 19 juin 1980 sur la loi applicable aux obligations contractuelles[21]. Selon la deuxième phrase de cet alinéa, le choix par les parties de la loi applicable au contrat « doit être exprès ou résulter de façon certaine des dispositions du contrat ou des circonstances de la cause »[22]. Ainsi, un choix (ou un consentement) peut être implicite et certain, mais est-il, dans le même cas, indubitable ?

Aussi bien l'article 8, alinéa 2, que l'article 7 de la directive passent outre à l'absence de consentement exprimé selon les exigences respectives de la lettre *a)* de chacune de ces dispositions. Suit, en effet, une série d'hypothèses dans lesquelles le traitement « est nécessaire » à l'un ou l'autre des objectifs énumérés. Sans revenir sur l'article 7,*f),* qui énonce cette nécessité en des termes vagues au point d'être indistincts, on se bornera aux hypothèses où il est permis de présumer un consentement implicite. C'est le cas de l'article 7, *b)* et de l'article 8, alinéa 2, *b).* Selon le premier de ces textes, il est dérogé à l'exigence d'un consentement si le traitement

> est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci.

Outre le contrat de travail, toute une gamme d'obligations contractuelles peut être envisagée : banque, assurance, transports, achat à crédit, emprunt, etc. Le concept de « nécessité » est, dans ce contexte, ambigu, car de tels contrats se sont, jusqu'à une époque récente, conclus et exécutés sans recours à un traitement informatisé, mais celui-ci est dorénavant requis par les techniques contemporaines de gestion des contrats. On conçoit malaisément que le client d'une banque ou d'une compagnie d'assurance, que le voyageur acquérant un billet d'avion exigent de leur cocontractant que toutes les informations relatives à ces opérations soient soustraites à un procédé d'enregistrement informatique. C'est en ce sens que le traitement de données à caractère personnel n'est pas seulement nécessaire, il est inéluctable, car celui qui prétendrait s'y soustraire se placerait en dehors de la vie sociale telle qu'elle est aujourd'hui organisée. Le degré et l'étendue de pareille nécessité ne sauraient être mesurés ni par un organe de contrôle ni 'par une juridiction, ils suivent inexorablement l'avancée des techniques et des pratiques informatiques.

L'article 8, alinéa 2 énumère cinq exceptions à la prohibition de traiter les données énumérées à l'alinéa 1er La lettre *b)* est rédigée dans les termes suivants:

> b) le traitement est nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail, dans la

---

[20] Mais le texte poursuit en ces termes : « Sauf dans les cas où la législation de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut être levée par le consentement de la personne concernée. »

[21] *JOCE*, NrL 266/1 du 9 octobre 1980. Le texte a été publié en six langues (allemand, anglais, français, italien, néerlandais et danois) dans: *BGBl,* 1986, II, S. 810.

[22] « The choice must be expressed or demonstrated with reasonable certainty by the terms of the contract or the circumstances of the case. » On peut hésiter sur le point de savoir si « reasonable certainty » est l'équivalent exact de : « de façon certaine ». Le texte allemand porte : « mit hinreichender Sicherheit ».

mesure où il est autorisé par une législation nationale prévoyant des garanties adéquates.

C'est donc ici un seul type de contrat qui est visé, le contrat de travail, et les précautions qui sont prises sont d'autant plus justifiées que la maîtrise de l'outil informatique vient renforcer le pouvoir traditionnellement exercé par le chef d'entreprise sur les travailleurs[23]. L'état de dépendance où se trouvent ceux-ci, état qui ne peut que s'aggraver à une époque où le travail devient de plus en plus rare, est considérablement accru par la masse d'informations aisément accessibles dont disposent aujourd'hui les entreprises informatisées. Toutefois les précautions ne concernent que le traitement des données sensibles. Pour les autres données, il suffit, aux termes de l'article 7, *b)*, que le traitement soit nécessaire. Mais on ne saurait, à cet égard, parler de révolution informatique, les instruments nouveaux se bornant à renforcer ou à rendre plus contraignant le lien de subordination qui demeure l'élément le plus caractéristique du contrat de travail. C'est donc aux lois organisant les relations de travail qu'il appartient d'établir les contrepoids rendus nécessaires par le surcroît d'efficacité conféré aux chefs d'entreprise.

Les règles de responsabilité

Les obligations mises à charge des responsables de traitements informatisés seraient de peu de poids si leur transgression ne devait entraîner des conséquences pour le contrevenant. Aux mesures administratives pouvant être arrêtées par l'autorité de contrôle et aux sanctions pénales que les États destinataires de la directive ont le devoir d'introduire dans leur ordre interne (art. 24) s'ajoute l'obligation de réparer le préjudice subi « du fait d'un traitement illicite ou de toute action incompatible avec les dispositions nationales prises en application de la présente directive » (art. 23, al. l[er]). Le régime de responsabilité ainsi institué est assez complexe et suscite une série de questions qui ne pourront qu'être succinctement évoquées.

Une première série de problèmes concerne la source du droit de la responsabilité. La directive se borne à énoncer un principe assorti d'une exception inscrite dans l'alinéa 2:

> Le responsable du traitement peut être exonéré partiellement ou totalement de cette responsabilité s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable.

On pourra se demander si la non-imputabilité est la seule cause d'exemption ou si d'autres exonérations de responsabilité peuvent être puisées dans le droit interne[24].

Pour le surplus, les conditions de la responsabilité doivent être déterminées selon le droit interne de chaque État, ce qui fait apparaître deux questions, la première étant relative au choix de la loi applicable (on y reviendra plus loin), la seconde au contrôle exercé par la Cour de justice des Communautés européennes sur le niveau minimum de responsabilité que les États doivent garantir. Or, comme le révèle la jurisprudence de la Cour, d'abord sur la responsabilité de la Communauté et ensuite sur celle des États, certaines notions fondamentales du

---

23 Damman et Simitis (n ote 17) donnent deux exemples d'hypothèses où l'enregistrement de données sensibles par l'employeur est licite : dans les entreprises de tendance et pour l'exécution de programmes visant à l'intégration des minorités (p. 164).

24 Selon Damman et Simitis (note 17), les États pourront soit régler la question dans l'instrument législatif donnant exécution à la directive, soit modaliser le droit commun de la responsabilité (p. 262). Après avoir affirmé que le régime de la directive se situe à mi-chemin entre la responsabilité pour faute et le système du risque (p. 262), ils énoncent ensuite plus précisément qu'il s'agit d'une responsabilité objective tempérée par la preuve de l'absence de faute (p. 263).

droit de la responsabilité varient selon les États, et il n'est pas certain que la Cour elle-même manie les concepts avec la rigueur souhaitable. Parmi les problèmes on citera la réparation d'un dommage indirect et celle du manque à gagner *(lucrum cessans).* En ce qui concerne le premier point, l'arrêt du 5 mars 1996 *(Brasserie du pêcheur / Factortame)* exige un lien de causalité direct entre la faute et le dommage, tandis que d'autres arrêts prononcés à la même époque et également relatifs à la responsabilité de l'État requièrent un lien de causalité sans plus, ce qui paraît inclure la causalité indirecte[25]. La mise en œuvre de l'article 23 de la directive suscitera un problème analogue.

Une dernière série de problèmes concerne la désignation du destinataire de l'obligation de réparer le préjudice. Selon les termes de la directive, c'est le « responsable du traitement », tel qu'il est défini par l'article 2, d) du même instrument. Mais il ne faudrait pas exclure les fautes personnelles d'individus ayant participé à la gestion du traitement ni celle de l'État s'il a été en défaut d'exécuter la directive ou en a fait une mise en œuvre incomplète ou incorrecte. Pareille respon sabilité est entrée dans le droit communautaire depuis l'arrêt *Francovich* du 19 novembre 1991 (cité à la note 1. ci-dessous).

LES CONFLITS DE NORME ET LEUR PACIFICATION

Vie privée et liberté d'expression

Parmi les dispositions de la directive qui, de manière explicite, posent les termes d'un conflit d'intérêts ou de valeurs que le législateur étatique — et, plus vraisemblablement, le juge — auront à tâche de surmonter, l'article 9 occupe une place de choix. Les « exceptions et dérogations » au chapitre II de la directive que les Etats membres peuvent prévoir « pour les traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique et littéraire » ne sont licites que « dans la seule mesure où elles s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression ». Sous sa forme classique, le conflit entre ce droit et cette liberté surgit quand un organe des médias a divulgué de manière illicite un fait relatif à la vie privée d'une personne. Dans l'article 9 de la directive, c'est d'un conflit au, second degré qu'il s'agit. Alors que l'élément de publicité est inhérent à l'atteinte à la vie privée et que de ce point de vue la récolte et le stockage d'informations dont la divulgation serait illicite ne sont pas par eux-mêmes illicites, c'est le traitement de telles données qui est visé par l'article 9. Sous couleur de faire une juste place à la garantie de la liberté d'expression, cette disposition pourrait y apporter une restriction nouvelle à travers le contrôle des sources des organes des médias. La différence est particulièrement notable en ce qui concerne les fichiers manuels qui entrent dans le champ d'application de la directive en vertu de l'article 3, alinéa 1er . Afin de pouvoir satisfaire à bref délai aux nécessités de l'information, les organes des médias et les agences de presse emmagasinent un grand nombre d'informations qui ont en partie pour objet la vie privée des personnes. Or, jusqu'à présent, il n'était pas illicite de recueillir et de stocker ces informations, la prudence des organes des médias ne devant s'exercer qu'à l'occasion de leur dissémination. Le lecteur des notices nécrologiques publiées par les grands journaux anglais à l'occasion du décès d'un personnage public (*public figure*) y trouvent des informations souvent circonstanciées relatives à la vie familiale et aux incartades

---

[25] CJCE 5 mars 1996, aff. jointes C-46/93 et C-48/93, *Brasserie du pêcheur* SA *et République fédérale d'Allemagne, The Queen and Secretary of State for Transport ex parte Factortame Ltd, Recueil* I-1131, § 65, p. 1152. Comp. CJCE, 19 novembre 1991, aff. jointes C- 6/90 et C-9/90, *Francovich et Bonifaci, Recueil* 1991, p. 5415, § 40 ; 14 juillet 1994, aff. C-91/92, *Faccini Dori, Recueil* 1-3325, p. 3357, § 27 ; 8 octobre 1996, aff. jointes C-178/94, C-179/94 et C-190/94, *Dillenkofer*, § 27, § 29. Pour plus de développements, voir F. Rigaux, « La responsabilité de l'État selon le droit des Communautés européennes », note sous l'arrêt du 5 mars 1996, *Rev. crit. jur. belge*, 1997, 283- 298.

sexuelles du défunt[26]. Il est vraisemblable que les règles sur ce point varient d'un pays à l'autre, notamment en raison du fait que, selon la tradition anglaise, le droit à l'honneur et à la vie privée est de nature strictement personnelle et s'éteint au décès de l'intéressé[27].

L'article 9 de la directive sera d'autant plus difficile à mettre en œuvre que la documentation accumulée par les organes des médias vise les personnages publics dont la vie privée est moins intensément protégée que celle des anonymes, sans qu'il soit aisé de circonscrire le « noyau dur » qui devrait être soustrait à toute divulgation.

L'article 9 de la directive est emblématique de la mission impossible assignée au législateur s'il faut par des normes générales concilier les deux libertés que la constitution de stocks de données à caractère personnel mettra nécessairement en conflit. La rigidité de la prévisibilité législative est inapte à embrasser des situations extrêmement diversifiées. D'où l'importance des arbitrages effectués par les autorités indépendantes de protection de la vie privée, grâce à l'adoption de codes de conduite ou de règles directrices *(guidelines),* sous la supervision finale des cours et tribunaux. Dans cette matière, au moins, la toute-puissance de la loi est un dogme dépassé. L'effort de conciliation requis par l'article 9 excède l'exercice traditionnel de la fonction législative : prononcer par voie de dispositions générales.

Droit communautaire et protection des droits de l'homme

Les « règles régissant la liberté d'expression » auxquelles se réfère l'article 9 de la directive appartiennent aussi et, même, au premier chef à un autre ordre juridique. Dans la mise en œuvre de toute la directive, mais spécialement de cet article, les États devront encore veiller au respect de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales. Sous quelque forme que ce soit, les dispositions qu'ils arrêteront pour donner exécution à la directive seront soumises au contrôle de la Cour européenne des droits de l'homme[28], et il existera dès lors deux juridictions internationales compétentes pour vérifier le respect par les États des obligations assumées dans deux ordres juridiques distincts. D'une part, la Cour de justice des Communautés européennes pourra être saisie, par la voie des questions préjudicielles de l'article 177 du traité CE, de toute question d'application ou d'interprétation de la directive et, le cas échéant, de l'action en manquement exercée par la Commission (ou par un autre État) si l'exécution donnée à la directive a été incorrecte ou incomplète. Mais la même exécution pourra aussi faire l'objet d'une requête introduite auprès de la Commission européenne des droits de l'homme[29], soit par la personne dont la vie privée aura subi une atteinte en raison de l'action ou de l'omission de l'État, soit par le journaliste, l'artiste, l'écrivain ou l'organe des médias dont la liberté d'expression aurait été injustement brimée. On notera au passage que l'accès direct à la Commission européenne des droits de

---

26 Voir à titre d'exemple la notice publiée par *The Times,* July 21, 1997, à l'occasion du décès de Sir James Goldsmith.

27 Voir notamment *: Report of the Committee on Privacy and Related Matters,* presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty, 1, June 1990, London, HMSO, dit Rapport Calcutt, du nom du président de la Commission, § 7.30 et 7.3 1. Le rapport ne conclut pas à l'opportunité du dépôt d'un projet de loi sur la *privacy* mais il y est annexé un appendice Q, *The Committees Proposed Code of Practice of the Press,* dont le § 16 est rédigé comme suit : « Newspapers should apply the same principles of accuracy, respect for privacy and non-discrimination to stories about the recently-dead as to stories about living ».

28 Tel qu'il sera organisé en vertu du Protocole n° 11 à la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, portant restructuration du mécanisme de contrôle établi par la Convention et de l'Annexe 9, faits à Strasbourg le 11 mai 1994. La loi belge du 27 novembre 1996 *(Le Moniteur belge,* 4 juillet 1997, p. 17855) a donné son assentiment à ce Protocole, et l'instrument de ratification a été déposé le 10 janvier 1997. Le Protocole entrera en vigueur le 1er novembre 1997.

29 Cela, jusqu'à l'entrée en vigueur du Protocole n° 11.

l'homme et, ultérieurement, à la Cour est ouvert à toute personne relevant de la compétence d'un État ayant adhéré à la Convention, tandis que les simples particuliers ne peuvent en général soumettre leurs griefs à la Cour de justice des Communautés européennes[30].

Sans que l'hypothèse d'un conflit entre les deux juridictions internationales ne puisse être totalement écartée, il est permis d'espérer une coordination des systèmes grâce à la qualification de « principes généraux du droit communautaire » attribuée par la Cour de justice aux dispositions de la Convention européenne et à la valeur interprétative qu'elle reconnaît aux décisions de la Cour européenne des droits de l'homme[31].

Ayant pour destinataires les États, la directive ne régit pas comme telle le traitement des données à caractère personnel par les organes de la Communauté elle-même. Aussi le traité d'Amsterdam du 2 octobre 1997 a-t-il prévu l'insertion dans le traité CE d'un nouvel article 286 (ex-article 213 B nouveau) rédigé dans les termes suivants :

> 1. À partir du 1er janvier 1999, les actes communautaires relatifs à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données sont applicables aux institutions et organes institués par le présent traité ou sur la base de celui-ci.
>
> 2. Avant la date visée au § 1, le Conseil, statuant conformément à la procédure visée à l'article [189 B], institue un organe indépendant de contrôle chargé de surveiller l'application des dits actes communautaires aux institutions et organes communautaires, et adopte toute autre disposition utile.

VI/ LA DÉTERMINATION DU DOMAINE SPATIAL DU NOUVEAU DROIT DE L'INFORMATIQUE

Qu'elles soient prises en vertu de la directive communautaire, qu'elles aient donné exécution à la Convention européenne du 28 janvier 1981 (dont la nature juridique est similaire à celle de la directive) ou qu'elles suivent les lignes directrices de l'OCDE, les législations nationales sur la protection des données à caractère personnel suscitent trois catégories de problèmes de conflit de lois.

Les législations spécialisées ont énoncé des règles nouvelles soumettant à des obligations administratives les entités et les personnes « responsables » du traitement de telles données, et elles ont institué une autorité publique nouvelle, généralement tenue pour une autorité publique indépendante[32]. A l'égard de ce premier aspect, le seul problème consiste à déterminer le domaine spatial d'application de cette partie de la loi.

Un second problème concerne le champ d'application des dispositions pénales, soit celles du droit commun, soit les incriminations spéciales prévues par les lois sur la protection des données. Dans les deux cas, et sauf si le législateur en a disposé autrement, il faut appliquer les règles de droit pénal international en vigueur dans l'État dont les tribunaux sont, le cas échéant, saisis d'une infraction.

---

[30] La demande de question préjudicielle est formulée par la juridiction nationale saisie d'un litige auquel une norme de droit communautaire est applicable, les parties à la cause ne pouvant que solliciter une telle mesure. Quant au recours de légalité de l'article 173 du traité CE, il n'est ouvert aux personnes physiques ou morales que dans l'hypothèse très exceptionnelle de l'alinéa 4.

[31] Sur le difficile problème des rapports entre les deux ordres juridiques, voir notamment : Commission européenne des droits de l'homme, 9 février 1990, *Rev. trim. dr. h.*, 1991, 395, et la note sous Cour européenne des droits de l'homme, 29 novembre 1992, *Rev. trim. dr. h.*, 1993, 335.

[32] Voir notamment F. Rigaux, op. cil. (n. 3, p. 26), n° 19.

Le traitement automatisé de données à caractère personnel met aussi en jeu des institutions traditionnelles du droit civil interne, notamment, comme on l'a vu, le contrat et la responsabilité. C'est à propos de ces institutions que se pose, dans les termes les plus classiques, un problème de conflit de lois, au sens du choix de la loi applicable à la situation.

La détermination du domaine spatial des lois étatiques conformément à l'article 4 de la directive

L'article 4 de la directive est, pour l'essentiel, resté fidèle au principe de territorialité, encore que ce principe soit d'application délicate à des opérations qu'il est aisé — et qu'il devient de plus en plus aisé — de délocaliser. C'est le lieu du traitement sur le territoire d'un État membre qui fixe le domaine d'application de la législation de cet État. Quand le traitement est réparti entre les établissements que le responsable maintient sur le territoire de plusieurs États membres, ce responsable doit veiller au respect, par chacun des établissements, des obligations prévues par la loi locale (art. 4, al. 1er, *a*). Comme le précisent les considérants (18) et (19) du préambule, l'harmonisation du droit en vigueur dans les États membres, finalité propre de la directive, a pour conséquence que le responsable du traitement n'a pas le devoir, et l'Etat sur le territoire duquel se trouve l'établissement principal n'a pas le pouvoir de vérifier selon la loi de cet État si la partie du traitement effectuée sur le territoire d'un autre État membre satisfait aux exigences de la loi du premier État.

Le principe de territorialité fait l'objet d'un rattachement alternatif: quand le responsable du traitement n'est pas établi sur le territoire de la Communauté, l'État membre sur le territoire duquel sont situés « des moyens, automatisés ou non » auxquels il est recouru pour le traitement a le devoir d'y appliquer ses dispositions protectrices (art. 4, al. 1er, *c*). Dans la même hypothèse, le responsable du traitement « doit désigner un représentant établi sur le territoire dudit État membre » (art. 4, al. 2).

Ce que la directive veut éviter par cette disposition est que des données recueillies sur le territoire d'un État membre puissent être traitées dans un État tiers hors de tout contrôle communautaire. C'est ainsi que le critère justifiant l'application du droit d'un État membre est tantôt le lieu de l'établissement ou des établissements du responsable du traitement, tantôt la localisation des moyens mis en œuvre dans le territoire de cet État par un responsable établi en dehors de la Communauté.

L'article 4, alinéa 1er, *b)* prévoit un autre critère justifiant l'application de la loi d'un État membre, à savoir la personnalité des lois. Selon le commentaire qu'en donnent Damman et Simitis (n. 1, p. 30), cette disposition viserait les traitements faits par les services diplomatiques d'un État membre sur le territoire d'un autre État membre. Le contrôle en serait soustrait à l'État territorial conformément à la Convention de Vienne sur les relations diplomatiques (p. 128-129).

Le champ d'application des incriminations pénales

L'article 24 de la directive fait une référence peu explicite aux « sanctions » que les États appliquent (et, sans doute, doivent appliquer) « en cas de violation des dispositions prises en application de la présente directive ». Le considérant (21) du préambule n'est guère plus explicite :

> (21) considérant que la présente directive ne préjuge pas les règles de territorialité applicables en matière de droit pénal.

À la vérité, le champ d'application du droit pénal n'est pas enfermé dans les « règles de territorialité ». Le principe de territorialité signifie d'abord que les juridictions répressives déterminent leur compétence en vertu des critères posés par la *lex fori* et qu'elles appliquent les incriminations et les peines prévues par la même loi. Toutefois la territorialité n'est pas le seul critère de la compétence pénale : une juridiction répressive peut être compétente en raison de la nationalité soit de l'auteur de l'infraction, soit de la victime. Si un tel délit a été commis à l'étranger, les incriminations et les peines sont déterminées par la *lex fori* sous réserve de la règle de la double incrimination : un fait ne peut être réprimé selon la *lex fori s'il* n'est pas punissable selon le droit du pays où il a été commis. Enfin, surtout à l'égard de comportements aussi difficiles à localiser que les traitements informatisés, le critère de territorialité est d'un maniement difficile et les hypothèses de plurilocalisation ne seront pas rares.

Les conflits de lois en matière de responsabilité civile et de contrat

L'article 23 de la directive impose aux États membres de garantir aux victimes d'un traitement illicite le droit d'obtenir la réparation de leur préjudice sans qu'il soit précisé en vertu de quelle loi pareille responsabilité sera déterminée. Quelques indications peuvent être données sur l'ampleur des problèmes : détermination du lien de causalité, étendue de la réparation, nature du dommage, admission ou non du dommage moral, du dommage émotionnel, du dommage par ricochet, perte du manque à gagner. Face à la diversité des solutions, le choix de la loi applicable revêt toute son importance,, mais il n'existe pas non plus, en la matière, de solution commune à tous les Etats membres. Sans doute l'application de la *lex loci delicti* est-elle assez généralement admise, mais, outre la difficulté de localiser le fait illicite, la règle elle-même s'accompagne d'exceptions et elle peut être évincée en vertu de l'exception d'ordre public. Quant à la localisation du fait, il semble que doive être préféré le rattachement « au lieu où les droits invoqués sont lésés, au domicile (ou à la résidence habituelle) de la victime »[33].

Le choix de la loi applicable au contrat suscitera moins d'hésitation parce que la plupart des États membres de l'Union européenne ont adhéré à la Convention de Rome du 19 juin 1980 sur la loi applicable aux obligations contractuelles. De plus, le droit des contrats n'a pas, dans l'économie de la directive et des méthodes actuelles de protection des données, une incidence aussi étendue que le droit de la responsabilité. Sans doute l'article 7 *b)* de la directive se réfère-t-il au contrat à l'exécution duquel un traitement informatisé est nécessaire, mais il est peu vraisemblable que la validité d'un tel contrat ou son interprétation soulève une question de conflit de lois préalable à l'application de la loi mettant en œuvre cette disposition.

Conclusion

Nul n'ignore que la directive 95/46 est le fruit d'efforts pénibles et soutenus, et il ne faut pas s'étonner que le texte issu de ce long travail pousse à l'extrême l'art de balancer des intérêts contradictoires et de dissimuler sous une phraséologie alambiquée les conflits qui ont divisé les rédacteurs eux-mêmes. Sans doute était-il impossible de faire mieux, mais la marge de manœuvre considérable laissée aux différents législateurs internes et l'impossibilité où se trouveront ceux-ci de fournir une copie beaucoup plus satisfaisante auront pour nécessaire conséquence que

---

[33] Pierre Bourel, « Du rattachement de quelques délits spéciaux en droit international privé », *Recueil des cours de l'Académie de droit international*, t. 214, p. 255-397, p. 338. Dans le même sens : F. Rigaux, *op. cit.* (n. 3, p. 28), n° 33, p. 472-473.

l'objectif d'harmonisation des droits en vigueur dans les États membres de l'Union européenne ne sera que partiellement atteint.

Force est de constater que la nature radicalement conflictuelle des intérêts mis en jeu par l'informatisation de la société, la diversité des situations manifestant de tels conflits et la volonté de tenir en équilibre des libertés fondamentales antagonistes résistent à l'énoncé de règles dessinant de manière précise et stable les procédés de solution de ces conflits. Mais il faut surtout dissiper la croyance illusoire en la possibilité de maintenir en équilibre les intérêts et les valeurs qui se font face. La justice ne manie pas une balance dont le fléau se tient de manière permanente en position horizontale. L'œuvre de justice consiste inéluctablement à faire pencher un des plateaux vers le bas et à hisser l'autre vers le haut. Selon les données et les circonstances propres à chaque espèce ou communes à une catégorie d'espèces[34], c'est tantôt une liberté tantôt l'autre qui l'emporte, et cette œuvre de justice ne saurait être accomplie par un législateur, et moins que tout par un instrument tenu de concilier les traditions juridiques d'un nombre croissant d'États[35]. Cela rend d'autant plus importante la fonction des autorités publiques investies du pouvoir de contrôler le respect effectif de principes formulés en termes nécessairement généraux et souvent ambigus. Et à la fin du jour il appartiendra aux tribunaux étatiques, aux juridictions constitutionnelles et aux deux Cours européennes de donner une consistance passagère aux mêmes principes et de vider les conflits qui les opposent les uns aux autres.

---

34 On aura reconnu la distinction entre deux méthodes de pondération des intérêts, le *categorical balancing* et *l'ad hoc balancing (Abägung im Einzelfall).*

35 Voir notamment: Pierre Legrand, « European Legal Systems are not converging », 45, ICLQ (1996), 52-81, et comp. plusieurs contributions de l'ouvrage collectif: *The Common Law of Europe and the Future of Legal Education,* ed. by Bruno De Witte and Caroline Forder (Metro, Kluwer, 1992).

CHAPITRE 10

La cryptographie

Mireille CAMPANA

Le principe historique de la cryptographie, qui est définie comme l'art d'écrire en éléments secrets, est la dissimulation du contenu d'une information au moyen d'un procédé connu de ses seuls utilisateurs.

Elle fournit deux grands types de services :

1 / ceux liés à la *confidentialité* des informations stockées ou échangées qui s'appuient sur la mise en œuvre de procédures de chiffrement ;
2 / ceux liés à *l'authenticité* des informations : intégrité du contenu et identification sûre de l'origine, qui recourent à des mécanismes dits « de signature électronique ». La signature numérique permet également d'assurer la « non-répudiation » de l'émission d'un message.

Les années 1990 ont été marquées par l'explosion des systèmes de communication, qui ont permis le développement des échanges électroniques, tant dans le domaine industriel et bancaire que dans celui du commerce en ligne et récemment celui des relations entre les citoyens et les administrations. Si, jusqu'à présent, l'ouverture et l' « interopérabilité » des réseaux et systèmes, ainsi que leurs performances, ont été privilégiées aux dépens de la sécurité, on assiste maintenant à une prise de conscience des problèmes par les acteurs de ces nouveaux réseaux, qui ont engagé des réflexions sur la sécurité et sur la cryptographie qui en constitue une brique fondamentale.

Longtemps réservée au domaine diplomatique et militaire, s'appuyant alors sur des principes mathématiques élémentaires, la, cryptographie a commencé à évoluer vers le milieu du siècle avec le début des télécommunications en intégrant essentiellement des techniques de codage de l'information ; mais il a fallu attendre les années 1970 pour qu'elle passe du secret des laboratoires militaires au domaine public, et s'institue comme une véritable science dans le domaine universitaire. Beaucoup d'articles ont alors été publiés et des conférences publiques ont été instituées. .

Des liens avec d'autres disciplines des mathématiques telles que codage et probabilités, arithmétique et géométrie algébrique, ont été établis. Cette évolution a été rendue nécessaire par le développement de l'informatique et des

télécommunications qui entraînait des besoins de protection pour tous; elle s'est accompagnée, dans certains pays, de la mise en place de législations et de réglementations qui pouvaient restreindre l'usage des procédés cryptographiques, dans le but de ne pas contrevenir aux besoins de la sécurité nationale et de la sûreté publique.

Ces législations, quand elles étaient explicites, ont pris des formes différentes, mais trois grandes tendances se sont dégagées : les pays qui n'effectuent en pratique aucun contrôle, comme l'Australie ou la Norvège ; les pays, les plus nombreux, parmi lesquels les États-Unis et la plupart des Etats européens, qui contrôlent uniquement l'exportation[1] des dispositifs cryptographiques et laissent la commercialisation et l'usage libres sur leur territoire ; enfin, les pays qui contrôlent l'usage et la commercialisation de ces dispositifs cryptographiques. La position américaine, qui s'appuyait sur le respect et la garantie de la protection individuelle mais aussi sur la libre entreprise, est en cours d'évolution ; même les contrôles portant sur les exportations sont actuellement remis en cause sous la pression des industriels exportateurs, et cet assouplissement sera vraisemblablement suivi par les autres pays.

Jusqu'à janvier 1999, la France a appartenu à la troisième tendance avec un système législatif et réglementaire très élaboré et fréquemment révisé, qui visait à obtenir un équilibre entre la protection des entreprises et des individus, d'une part, les obligations liées à la sécurité de l'État, d'autre part. La dernière législation (loi de réglementation des télécommunications de 1996 complétée par des décrets de 1998) mettait en place un système reposant sur un emploi libre des produits de force limitée[2] ou utilisant des clés qui pouvaient permettre à l'administration la récupération des données *a posteriori* dans certaines conditions.

Cet ensemble complexe de décrets et d'arrêtés était prévu non seulement pour pouvoir facilement s'adapter aux besoins du marché et aux progrès de la technologie, mais aussi pour permettre un changement de position politique sur le contrôle ; il a permis à la France de passer très rapidement, et sans avoir à légiférer, de la troisième à la deuxième tendance (dans la pratique, sinon formellement dans les textes) en relevant de 40 à 128 bits la longueur de clé des produits de cryptographie, par deux décrets simples (n^{os} 99-199 et 99-200 du 17 mars 1999). Ces décisions revenaient à accorder la liberté d'utilisation à la quasi-totalité des dispositifs cryptographiques (en particulier des produits dits

[1] Les règles applicables à l'exportation des cryptographiques qui sont considérés comme des « biens à double usage » (usage civil et usage militaire) sont définies dans le cadre des arrangements de Wassenaar de juillet 1996, plusieurs fois révisés par la suite ; ils concernent la plupart des pays industrialisés. Ces règles sont appliquées plus ou moins sévèrement selon les pays.

[2] Bien que les réalités techniques puissent être parfois différentes, il est souvent d'usage d'évaluer l'efficacité de la protection que procure un dispositif en fonction de la taille de sa clé. On verra la signification de ce paramètre dans la description des techniques.

« forts »). En outre, les formalités administratives sont allégées pour les utilisateurs ; elles ne pèsent plus que sur les fournisseurs qui doivent, pour commercialiser leurs produits, effectuer une déclaration auprès du SCSSI[3] à laquelle est jointe un dossier technique décrivant le produit.

Une nouvelle législation est en cours d'élaboration ; elle devrait prendre en compte de nouveaux besoins apparus avec le développement du commerce électronique, comme les signatures dématérialisées.

LES TECHNIQUES

Des procédés secrets, on a évolué vers des algorithmes mathématiques connus utilisant des paramètres secrets que l'on a nommés « clés ». Actuellement, la cryptographie classique (dite symétrique ou à clé secrète) repose sur ce principe. Pour chiffrer un message, on utilise un algorithme répertorié ou correspondant à un standard[4] s'appuyant sur un paramètre secret, la clé, qui est un *nombre* connu des différents interlocuteurs. Il est relativement facile de construire de tels algorithmes et seuls les besoins d'interopérabilité des systèmes de cryptographie limitent leur nombre. Les États-Unis, dans les années 1970, ont tenté d'imposer un algorithme, unique, baptisé DES *(Data Encryption Standard)*, en insistant sur les problèmes d'interopérabilité et aussi de sécurité et d'économie. Pour cela, le département du Commerce a fait réaliser par la Société IBM un algorithme qui devait être publié, de manière à permettre son évaluation par tous, et qui devait être libre de tous droits d'usage. Plus de vingt ans après, la seule faiblesse révélée de cet algorithme est la longueur de la clé (56 bits), jugée trop courte pour les moyens de calcul actuels (6).

Même si le DES n'a jamais obtenu le statut de norme internationale, essentiellement pour des raisons politiques car certains États s'opposaient alors à la prolifération de dispositifs cryptographiques, il a été pendant des années l'algorithme employé de façon systématique dans le domaine commercial et reste aujourd'hui le plus employé. Il a quelques concurrents, essentiellement dans le domaine des produits logiciels, comme le *RC*4 ou *IDEA*, qui sont mieux adaptés à des implantations logicielles. Les applications gouvernementales utilisent pour des raisons de sécurité des algorithmes non publiés; il en va de même dans le domaine des télécommunications où les opérateurs ont en général préféré définir leurs propres normes[5].

[3] Service central de la sécurité des systèmes d'information chargé de l'application de la réglementation. Avant mars 1999, la commercialisation et l'utilisation de tout dispositif cryptographique étaient soumises à autorisation de ce service. C'est toujours le cas pour les dispositifs dont la taille des clés servant au chiffrement d'information dépasse 128 bits.

[4] La fonction est a priori connue de tous; on verra plus loin les exceptions à cette règle.

[5] Ces normes ne sont pas toujours publiées ; cependant, dans la mesure où elles ont vocation à être fournies aux différents constructeurs dans tous les pays, leur caractère confidentiel peut être considéré comme relatif.

Il existe deux systèmes de chiffrement.

Les systèmes de chiffrement à clé secrète, ou systèmes symétriques

Ils reposent sur le partage entre deux interlocuteurs en communication, d'une même clé secrète S qui sert à paramétrer un algorithme à la fois pour *le chiffrement d'un message et pour son déchiffrement.* La clé S doit faire l'objet d'un échange physique préalablement à toute communication. Pour le stockage de messages, le principe est le même avec un seul interlocuteur. Cette clé prend en général la forme d'un ensemble de bits de taille limitée. Un procédé, connu sous le nom d' « attaque par force brute », utilisé pour retrouver le contenu des communications, consiste à essayer toutes les clés possibles[6]. Leur nombre dépend de la taille de ces clés : pour une clé de n bits, il y a 2^n clés possibles ; la complexité d'un produit est donc bornée par la taille de cet ensemble.

En général, la clé secrète commune S n'est pas utilisée directement pour chiffrer les messages, mais pour chiffrer une autre clé K qui est un nombre tiré au hasard par l'émetteur à chaque session et qui sert comme clé secrète pour chiffrer les messages. Cette clé K chiffrée est envoyée en début de session ou de message ou, dans le cas de stockage, conservée avec le message.

Les systèmes à clé publique ou systèmes asymétriques

Les algorithmes à clé publique servent à chiffrer des messages, mais aussi à calculer des signatures numériques. Une signature numérique est une valeur qui dépend du message, considéré alors sous sa forme numérisée comme un nombre, et de l'identité du signataire, qui doit être le seul à pouvoir calculer cette signature. Un message signé est composé du message en clair et de cette signature numérique. Vérifier une signature consiste, en appliquant la fonction inverse de la signature, à retrouver le message en clair.

Chaque utilisateur possède son propre couple de clés différentes S et P :

La clé S est gardée *secrète* par son propriétaire qui l'utilise pour *déchiffrer* des messages reçus ou *signer* des messages.

---

[6] La complexité de cette attaque par force brute dépend de la vitesse d'exécution de l'algorithme et de la puissance de calcul utilisée ; à titre indicatif, pour certains algorithmes courants type DES, il est possible de retrouver une clé de 40 bits en quelques heures ou dizaines d'heures de PC. Cette complexité est multipliée par un facteur 65 000 si l'on passe à 56 bits ; pour 128 bits, effectuer ce type de recherche exigerait des ressources très largement non disponibles à l'heure actuelle.

La clé P est rendue *publique*. Elle dépend de la clé S par une fonction à sens unique : la fonction est facilement calculable, mais son inversion est extrêmement difficile (on ne sait pas déduire S de P). Elle sert à quiconque pour *chiffrer* les messages destinés au propriétaire du couple de clés, ou à *vérifier* les signatures.

Pour chiffrer un message destiné à une personne A, le correspondant B applique la fonction définie par P_A, la clé publique de A. A le déchiffrera avec sa clé secrète S_A qu'elle est seule à détenir.

Pour signer un message, B lui applique la fonction définie par sa clé secrète *SB* pour calculer une signature. Pour vérifier cette signature, A lui applique la fonction inverse de la fonction de signature, définie par la clé publique P_B de B, ce qui lui permet de retrouver en clair le message initial. Seul B, qui détient S_B, a pu calculer cette signature.

B envoie un message chiffré et/ou signé à A	
B chiffre avec P_A	A déchiffre avec S_A
B signe avec S_B	A vérifie avec P_B

Comme les algorithmes à clé publique sont lents à exécuter, on chiffre toujours les messages avec des algorithmes à clé symétrique, et on utilise le dispositif à clé asymétrique pour chiffrer la clé de session générée aléatoirement, comme dans le cas des systèmes à clé secrète.

Relation entre la clé publique et son détenteur

Le problème fondamental que pose l'utilisation de la clé publique peut se définir ainsi: comment établir un lien sûr entre une clé publique P_A et son détenteur A ? Il est absolument fondamental pour l'émetteur du message de pouvoir être sûr que la clé publique qu'il utilise pour chiffrer un message, destiné à A, est bien celle de A. De la même façon, pour vérifier les messages signés par A, il faut être sûr du lien entre A et la clé publique P_A qui sert à vérifier les signatures. Les inventeurs[7] du concept de clé publique préconisaient l'utilisation d'annuaires de clés publiques utilisant des supports non modifiables (papier ou support magnétique non « ré-inscriptible »).

Il est possible également d'utiliser des certificats créés par des *autorités de certification*, et c'est la solution retenue à l'heure actuelle. Un utilisateur A présente sa clé publique P_A à une telle autorité, qui possède elle-même un couple

[7] Diffie et Helleman, qui ont formalisé pour la première fois en 1977 le concept de chiffrement asymétrique et proposé un schéma d'échange de clés reposant sur ce concept.

(P_{aut}, S_{aut}) ; P_{aut}, est supposée connue de tous. L'autorité vérifie l'identité de A et signe avec sa clé secrète l'ensemble constitué de l'identité et de la clé publique de A, à savoir : Certificat = Signature $_{Saut}(ID_A, P_A)$ où ID_A désigne l'identité de A.

Seule l'autorité peut calculer des certificats vérifiables avec P_{aut} en signant des ensembles identité-clé publique.

Les *certificats* peuvent être placés dans un annuaire qui ne requiert pas de sécurité particulière. Lorsque A émet un message signé avec S_A, il l'accompagne de son certificat (ou le destinataire retrouve celui-ci dans l'annuaire). Pour vérifier la signature émise par A, le destinataire B, qui dispose de la clé publique de l'autorité P_{aut}, (supposée connue de tous), peut vérifier le certificat de A, c'est-à-dire retrouver l'ensemble (ID_A, P_A) et acquérir la certitude que P_A correspond bien à A ; il utilise ensuite P_A pour vérifier la signature du message émis par A.

Le concept de clé publique a remis en cause les architectures traditionnelles d'organisation de la cryptographie. L'utilisation de schémas à clé secrète permet de définir des groupes d'utilisateurs appelés généralement réseaux qui partagent un même secret et l'utilisent pour communiquer entre eux de manière sécurisée. L'utilisation de procédés à clé publique n'implique aucun partage de secret entre les utilisateurs mais implique l'existence d'une autorité de certification appelée souvent tiers de confiance qui va forger les certificats, assurant le lien entre les identités des personnes et de leurs clés publiques.

La sécurité de tout le système dépend du niveau de sécurité offert par cette autorité, et il est fondamental que cette autorité s'assure de l'identité d'un utilisateur avant de lui délivrer un certificat. Le niveau de confiance que l'on peut accorder au certificat est directement lié au sérieux avec lequel l'autorité de certification s'est assurée de l'identité de la personne, et aussi de la sécurité de la procédure de calcul des certificats. En particulier, la protection de la clé secrète de l'autorité est particulièrement importante, puisque c'est elle qui permet de fabriquer les certificats. Elle ne doit donc pas être accessible. Il est également important de définir des durées de validité pour les certificats. Des « profils de protection » qui sont des politiques de sécurité type ont été rédigés et validés par des groupes de travail impliquant tous les acteurs concernés (organismes institutionnels, bancaires, industriels…).

Le rôle de l'autorité de certification peut ou non comprendre la génération du couple de clés. Dans le premier cas, elle peut alors servir de tiers de recouvrement ou des clés ou même du contenu en clair des messages chiffrés, c'est-à-dire que, étant également détenteur de la clé secrète, elle a la possibilité, pour certains types de dispositifs, de retrouver le contenu d'un message chiffré, par exemple pour répondre à une demande d'un juge (ce rôle avait été envisagé dans la législation mise en place en 1996).

Il est également possible d'envisager des hiérarchies d'autorités ou des croisements lorsqu'elles se certifient entre elles afin de permettre à des utilisateurs dépendant d'autorités différentes de communiquer entre eux.

LES APPLICATIONS EXISTANTES

À l'exception de quelques secteurs comme le secteur bancaire[8] en France ou plus récemment le secteur de la Santé, la cryptographie n'est pas à l'heure actuelle largement répandue dans les applications ; les législations restrictives ont souvent été mises en cause mais il ne faut pas méconnaître les difficultés liées à la mise en œuvre. Même dans les pays où il n'y a pas de contrôle à la fourniture et à l'utilisation des produits de cryptographie comme les États-Unis, il existe bien une offre de tels produits, surtout dans le domaine de l'Internet[9]. Mais ceux-ci ne sont généralement pas massivement employés. Il existe également des actions pour définir des standards d'algorithmes (comme le DES, mais aussi son remplaçant en cours de définition, l'AES — pour *Advanced Encryption Standard),* ou plus récemment des standards de protocoles (comme *IPSEC,* norme de chiffrement au niveau IP ou S/MIME pour le chiffrement de la messagerie).

Mais le caractère non obligatoire et souvent non définitif de ces standards (généralement présentés sous forme de *Request for Comments* par l'IETF) rend les industriels circonspects, et les produits ne sont pas toujours disponibles.

Par ailleurs, une fois un produit choisi, les difficultés liées à l'administration de la cryptographie, en particulier à la gestion des clés secrètes ou publiques, deviennent vite considérables dès que le nombre d'utilisateurs augmente ou que l'on veut toucher des populations diverses ou dispersées. Il n'est pas non plus évident de définir des supports protégés pour stocker les clés secrètes, en dehors des cartes à microprocesseur qui ne s'adaptent d'ailleurs pas à tous les postes de travail. Enfin, s'il est possible de placer des mécanismes cryptographiques à divers niveaux (sur les liens physiques, dans le réseau ou dans les couches logicielles applicatives), ceux-ci ne sont pas forcément transparents. La mise en place de services de chiffrement peut gêner certains

[8] L'ensemble du secteur bancaire français regroupé au sein du GIE Cartes bancaires a mis en place des procédures de retrait et de paiement sécurisées s'appuyant sur le choix de dispositifs sécurisés (cartes à microprocesseur) et l'utilisation de protocoles cryptographiques, ce qui a permis d'obtenir un taux de fraude très largement inférieur à ceux des autres pays, tout en assurant l'interopérabilité du dispositif.

[9] S'il est relativement facile d'intégrer des services de chiffrement pour les échanges de données, en particulier quand cette intégration se fait dans les couches logicielles, chiffrer la voix est beaucoup plus délicat, et l'offre dans ce domaine est particulièrement restreinte et coûteuse. La téléphonie sur IP permettra peut-être de régler le problème, mais l'offre n'est pas encore mûre dans ce domaine.

services d'administration du réseau, voire le fonctionnement de protocoles de communications lorsqu'il s'agit de téléphonie.

Il y a cependant des domaines où la mise en place d'une protection du contenu des informations échangées conditionne celle des applications (les récentes révélations sur le système *Échelon* ont montré la réalité des menaces liées aux interceptions sur les réseaux publics). La *confidentialité* n'est pas le seul service nécessaire : c'est le cas en particulier du commerce électronique où l'on recherche *l'authenticité* d'une transaction mais aussi des procédures dématérialisées entre le citoyen et l'État ou les organismes sociaux.

Dans le cas d'une déclaration de revenus dématérialisée, par exemple, il est indispensable de pouvoir garantir l'identité de l'émetteur et l'intégrité des données transmises. Le secteur de la Santé a été le premier à se lancer dans la mise en place d'une telle procédure à grande échelle, à savoir la transmission électronique des feuilles de soin qui a fait intervenir une multiplicité d'intervenants (ministère, caisses d'assurance maladie, Ordre des médecins). Le volume des transactions, les enjeux financiers, les problèmes liés à l'éthique et au secret médical ont induit de très fortes contraintes de sécurité sur le réseau, les logiciels applicatifs et les dispositifs (carte de professionnel de santé et carte patient). Le ministère a fait le choix d'une *architecture à clé publique* et a mis en place une infrastructure de gestion de clés très complexe, qui est la plus importante application déployée à l'heure actuelle. Ce dispositif permet également de sécuriser les transactions entre professionnels de santé.

Au-delà de ces grands déploiements, l'entreprise qui veut sécuriser son système d'information, ou les *particuliers qui désirent sécuriser* leurs données et leurs échanges, peuvent maintenant disposer de produits ergonomiques intégrés dans des logiciels grand public, comme les navigateurs, ou s'en procurer sur le Web, comme le célèbre PGP *(Pretty Good Privacy).* Ce logiciel, développé à l'origine par un chercheur américain, Phil Zimmerman, avait pour but de mettre à la disposition de chacun les sources d'un système entier de chiffrement. Il s'est enrichi au cours des années en conservant cet esprit d'ouverture (libre disponibilité des sources) que l'on retrouve dans *Linux. Il* est cependant plus adapté à un *fonctionnement de proximité* (on reconnaît les clés de ses amis et des amis de ses amis) qu'à des applications d'achat et de paiement « impulsifs » sur Internet.

Enfin, si la *cryptographie* est l'une des briques de base de la sécurité, la plus médiatisée eu égard au secret qui a longtemps dissimulé son développement et la mieux construite, puisqu'on peut l'apparenter à une branche des mathématiques, *elle ne peut à elle seule résoudre tous les problèmes de sécurité.* Quelle que soit la force d'un algorithme ou la longueur des clés employées, il peut y avoir des problèmes d'implantation (voulus ou non) dans un dispositif, qui font qu'il est possible de retrouver les informations protégées par un moyen détourné (lorsque ces « problèmes » sont volontaires, on les désigne sous le nom de *backdoors).* Une

démarche d'évaluation des produits cryptographiques, prenant en compte non seulement la complexité cryptographique mais aussi les modes d'implantation, vient de démarrer sous l'égide du Secrétariat général de la Défense nationale (SGDN), mais c'est une tâche très lourde, en raison du volume et de la complexité des logiciels.

Par ailleurs, *la cryptographie ne protège pas les systèmes:* lorsqu'un poste de travail situé sur un réseau local établit une connexion avec le monde extérieur, même si cette connexion est protégée, elle peut être utilisée depuis l'extérieur pour effectuer des intrusions sur les machines de ce réseau local, en extraire des informations ou en détruire. Il faut mettre en place des barrières (en général désignées sous le nom de *firewalls)* comportant des filtres et des antivirus. Enfin, le problème de la connexion à l'Internet d'un poste comportant sur son disque des données confidentielles, même stockées chiffrées, est extrêmement difficile à résoudre.

ANNEXE. - Exemples de logiciels de protection couramment utilisés

Jacques Roure

Commerceserver/400 - Serveur SHTTP **Pour** IBM AS/400, sécurisation des transactions sur Internet.

Fols-Security - Gestion d'accès d'un client aux services d'un serveur,SEMA-GROUP.

Raptor Firewall - Constitue une solution *firewall* pour réseaux *corporate,* LAN2LAN, l'interconnexion Intranet ou l'accès à Internet.

Security Box SHL - Solution de sécurité globale pour Internet Intranet Extranet, confidentialité, authentification, intégrité.

Websentry - Autorise un accès sécurisé au Web (contrôle d'accès, chiffrement), aux applications *mainframe (Bull,* IBM, Unix) et multimédia.

Webaccess & Webcontrol - Accès sécurisé et contrôlé aux ressources d'Internet sans y raccorder le réseau de l'entreprise.

Webcard - Contrôle des accès à Internet. Gestion des temps de connexion. Pilotage de carte à puce.