LA PROTECTION DE LA VIE PRIVEE AU REGARD DES DONNEES INFORMATIQUES *

Emmanuel DECAUX
Professeur à l'Université Panthéon-Assas Paris II

La notion de vie privée – de « *privacy* » que le mot « intimité » rend mal, à défaut du vieux « priveté » mentionné par Littré – est au cœur de la philosophie libérale, avec la distinction de la sphère publique et de la sphère intime. Cette notion n'apparaît pourtant pas en tant que telle dans la Déclaration des droits de l'homme et du citoyen de 1789, reflétant ainsi l'opposition établie par Benjamin Constant entre la « liberté des anciens » et la « liberté des modernes » qui préfigure le distinguo classique d'Isaiah Berlin[1]. Il y aurait sans doute un parallèle à prolonger entre les libertés anglaises et la Liberté française…

« *Notre liberté, à nous, doit se composer de la jouissance paisible de l'indépendance privée* » réclamait Benjamin Constant dans son fameux discours prononcé à l'Athénée de Paris en 1819, à défaut d'une souveraineté trop souvent illusoire[2]. Après lui, les doctrinaires – le plus souvent anglophiles – comme Royer-Collard, invoqueront « *le mur de la vie privée* », selon une formule dont la paternité sera disputée[3]. Il est significatif que comme l'article 76 de la Constitution de Frimaire an VIII (1799), la Constitution de 1848 précise que « *la demeure de toute personne habitant le territoire français est inviolable ; il n'est permis d'y pénétrer que selon les formes et dans les cas prévus par la loi* » (art. 3). Des dispositions ponctuelles viseront à protéger le « secret » de la vie privée, en matière de presse avec une loi de 1868. Mais c'est bien plus tard que l'article 9 du Code civil – introduit par la loi du 17 juillet 1970 – viendra consacrer formellement le principe en vertu duquel « *[c]hacun a droit au respect de sa vie privée* »[4].

Le Conseil constitutionnel considèrera pour sa part, de manière très allusive, que *« la liberté individuelle constitue l'un des principes fondamentaux garantis par les lois de la*

---

* Intervention faite à Belfast, en avril 2007, à l'occasion d'une journée d'étude sur la vie privée de l'Association des juristes franco-britanniques.

[1] Sir Isaiah BERLIN, *Two Concepts of Liberty,* Oxford, Clarendon Press, 1958.

[2] Benjamin CONSTANT, *De la liberté chez les Modernes*, présenté par Maurice GAUCHET, Paris, Hachette, coll. Pluriel, 1980, p. 501.

[3] Le dictionnaire d'Emile Littré, au bénéfice d'une lettre de Stendhal, attribue la formule à Talleyrand.

[4] *Cf.* « Vie privée » par Emmanuel DREYER, in *Dictionnaire des droits fondamentaux*, sous la direction de Dominique CHAGNOLLAUD et de Guillaume DRAGO, Paris, Dalloz, 2006, p. 726. Et plus généralement, Pierre KAYSER, *La protection de la vie privée par le droit*, Economica / Presses universitaires d'Aix-Marseille, 3° éd., 1995.

République » pour limiter la fouille des véhicules[5] En 1995, s'agissant de vidéosurveillance, il estimera expressément cette fois que « *la méconnaissance du droit au respect de la vie privée peut être de nature à porter atteinte à la liberté individuelle* »[6].

Dans le même temps, la protection de la vie privée est pleinement consacrée par tous les grands textes internationaux, à l'instar de l'article 12 de la Déclaration universelle de 1948 : « *Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes* ». C'est le cas également de l'article 8 de la Convention européenne des droits de l'homme – qui sera la matrice d'une jurisprudence abondante et riche – comme de l'article 17 du Pacte international relatif aux droits civils et politiques – qui a fait l'objet de l'Observation générale n° 16 (1988).

Toutefois ces principes classiques qui supposent une non-ingérence, une « abstention » de l'Etat, ne sont pas suffisants pour protéger l'individu face au développement de l'informatique. C'est le sens de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés qui a institué en France un régime particulièrement protecteur, en instituant la *Commission nationale de l'informatique et des libertés* (CNIL). Cette grande loi reste la base du système français, même si elle a été révisée à plusieurs reprises, notamment avec la loi du 7 août 2004 « relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés »[7].

Une des principales caractéristiques du système français est l'interdiction « *de collecter et de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuse ou l'appartenance syndicale des personnes ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci* » (art. 8-1). Cette interdiction de principe comporte quelques exceptions, au bénéfice des églises, des partis ou des associations qui peuvent constituer un fichier de leurs membres, avec l'accord de ces derniers, ainsi que dans un but d'intérêt général, s'agissant notamment de la gestion des services de santé. Mais un organisme officiel comme l'Institut national de la statistique et des études économiques (INSEE) ne peut établir de statistiques ethniques, ainsi que la CNIL vient de le confirmer. Des dérives restent toujours possibles, dans certaines municipalités, notamment à des fins électorales.

---

[5] Décision n° 76-75 DC du 12 janvier 1977, n° 24 *in* Louis FAVOREU et Loïc PHILIP, *Les Grandes décisions du Conseil constitutionnel,* 13° éd., Paris, Dalloz, 2005.

[6] Décision n° 94-352 DC du 18 janvier 1995. *Cf.* aussi la décision n° 2004-499 DC du 29 juillet 2004 sur les données personnelles, à l'occasion de la loi du 7 août 2004 (cf. *infra*). Le texte des décisions du Conseil constitutionnel est disponible sur son site à l'adresse : www.conseil-constitutionnel.fr.

[7] JO n° 182 du 7 août 2004, p. 14063. *Cf.* Legifrance (www.legifrance.gouv.fr) ou le site de la CNIL (www.cnil.fr).

Parallèlement la loi française fixe un régime souple, prévoyant que *« les données sont collectées et traités de manière loyale et licite* » et ce « *pour des finalités déterminées, explicites et légitimes* », qu'elles « *sont adéquates, pertinentes et non excessives »* au regard de ces finalités. Il importe également qu'elles soient « *exactes, complètes et, si nécessaire, mises à jour* », des mesures devant être prises « *pour que les données inexactes ou incomplètes […] soient effacées ou rectifiées* » (art. 6). La règle du consentement de la personne concernée prime, ou à défaut « *le respect d'une obligation légale incombant au responsable du traitement* », « *l'exécution d'une mission de service public* » ou encore « *la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentales de la personne concernée* » (art. 7). Les mots parlent d'eux-mêmes : « loyauté », « licéité », « légitimité », « adéquation », « pertinence », « proportionnalité », tout est matière d'interprétation. En dehors de quelques interdictions absolues, la loi s'en tient à la recherche permanente de l'équilibre, du raisonnable et du relatif, sous le contrôle de la CNIL.

Une dynamique a également été créée depuis les années soixante-dix, d'abord sur le terrain du droit comparé, avec de nombreuses législations protectrices, la loi adoptée par le Land de Hesse en 1974 jouant le rôle de pionnier. Parfois le principe est même consacré dans les nouvelles constitutions démocratiques, comme en Espagne, avec l'article 18 § 4 de la Constitution de 1978 qui précise que « *la loi limitera l'usage de l'informatique pour garantir l'honneur et l'intimité personnelle et familiale des citoyens et le plein exercice de leurs droits* », ou au Portugal avec la Constitution de 1976 dont l'article 35 sur « *l'utilisation de l'informatique* » a été complété lors des révisions constitutionnelles de 1982 et 1989. On retrouve la même dynamique sur le plan international et notamment européen, avec des conventions et des directives visant à établir un système protecteur transfrontière, comme on le verra.

C'est dire l'importance de la Charte des droits fondamentaux de l'Union européenne, proclamée à Nice en 2000, qui vient compléter un article 7, tout à fait classique, consacré au « *respect de la vie privée et familiale* », par un article 8 inédit sur la « *protection des données à caractère personnel* » qui se fonde sur l'article 286 du Traité instituant la Communauté européenne. En vertu de l'article 8 de la Charte :

> « *1. Toute personne a droit à la protection des données à caractère personnel le concernant.*
> *2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.*
> *3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante* »[8].

[8] Guy BRAIBANT, *La Charte des droits fondamentaux de l'Union européenne*, Paris, Le Seuil, coll. Points, 2001. *Cf.* aussi le commentaire de l'article II-68 par Olivier de SCHUTTER, in *Traité établissant une Constitution pour l'Europe*, *Partie II, La Charte des droits fondamentaux de l'Union*, tome 2, sous la direction de Laurence BURGORGUE-LARSEN, Fabrice PICOD et Anne LEVADE, Bruxelles, Bruylant, 2005, p. 122.

Ces dispositions générales traduisent une véritable révolution juridique dans la conception même des droits de l'homme. Il s'agit d'abord de protéger la vie privée et pas seulement de la « respecter » à travers une simple non-ingérence. On retrouve le triptyque mis en avant par A. Eide : respecter, protéger et mettre en œuvre (*respect, protect and fulfill*). Cela implique des obligations positives de l'Etat, notamment en déterminant un cadre juridique protecteur qui vise tous les acteurs potentiels, acteurs publics mais aussi acteurs privés. Enfin l'idée de confier un rôle de protection à une autorité administrative indépendante est également très novatrice, par rapport à la conception traditionnelle qui fait de « l'autorité judiciaire [la] gardienne de la liberté individuelle », comme le rappelle l'article 66 de la Constitution française.

Sans entrer dans des détails techniques – ce dont nous serions d'ailleurs bien incapable – nous voudrions tenter de voir comment, depuis une trentaine d'années, un cadre européen protecteur a été mis en place sur la base de ces grands principes (I) avant de nous interroger sur la solidité de ce dispositif face aux nouveaux défis aussi bien techniques que politiques apparus dans les dernières années (II).

I. – LA CONSTRUCTION D'UN CADRE JURIDIQUE PROTECTEUR

Des travaux importants ont été entrepris au sein des Nations Unies pour élaborer des principes directeurs en matière de protection des données, grâce à l'impulsion de Louis Joinet désigné comme rapporteur spécial en 1980 par la Sous-Commission de la promotion et de la protection des droits de l'homme (résolution 12 XXXIII), après avoir été conseiller juridique de la CNIL. Ils ont abouti à des « *principes directeurs pour la réglementation des fichiers informatisés concernant des données à caractère personnel* » entérinés par la Sous-Commission de la promotion et de la protection des droits de l'homme dès 1983[9], puis adoptés par l'Assemblée générale des Nations Unies dans sa résolution 45/95 du 14 décembre 1990. On retrouve une série de « *principes concernant les garanties minimales qui devraient être prévues dans les législations nationales* », notamment le principe de licéité et de loyauté, le principe d'exactitude, le principe de finalité, le principe d'accès par les personnes concernées, le principe de non-discrimination, le principe de sécurité, assortis de mécanismes de contrôle et de sanctions. Ainsi, « *chaque législation devrait désigner l'autorité qui, en conformité avec le système juridique interne, est chargée de contrôler le respect des principes précités. Cette autorité devrait présenter des garanties d'impartialité, d'indépendance à l'égard des personnes ou organismes responsables des traitements et de leur mise en œuvre, et de compétence technique* » (principe 8). Par ailleurs, la résolution vise l'application de ces principes directeurs aux fichiers détenus par les organisations internationales, la question déjà sensible dans le cas d'Interpol l'est plus encore aujourd'hui s'agissant des listes établies par le comité contre le terrorisme du Conseil de sécurité.

[9] E/CN.4/Sub.2/1983/18.

Se fondant lui aussi très largement sur l'étude menée à bien par Louis Joinet dans le cadre de la Sous-Commission, le Comité des droits de l'homme dans son Observation générale n° 16 de 1988 souligne que « *le rassemblement et la conservation, par des autorités publiques, des particuliers ou des organismes privés, de renseignements concernant la vie privée d'individus sur des ordinateurs, dans des banques de données et selon d'autres procédés, doivent être réglementés par la loi. L'Etat doit prendre des mesures efficaces afin d'assurer que ces renseignements ne tombent pas entre les mains de personnes non autorisées par la loi à les recevoir, les traiter et les exploiter, et ne soient jamais utilisées à des fins incompatibles avec le Pacte. Il serait souhaitable, pour assurer la protection la plus efficace de sa vie privée, que chaque individu ait le droit de déterminer, sous une forme intelligible, si des données personnelles le concernant et, dans l'affirmative, lesquelles, sont stockées dans des fichiers automatiques de données, et à quelles fins. Chaque individu doit également pouvoir déterminer les autorités publiques ou les particuliers ou les organismes privés qui ont ou peuvent avoir le contrôle des fichiers le concernant. Si ces fichiers contiennent des données personnelles incorrectes ou qui ont été recueillies ou traitées en violation des dispositions de la loi, chaque individu doit avoir le droit de réclamer leur rectification ou leur suppression* » (§ 10)[10].

Mais c'est évidemment dans le cadre européen que les efforts les plus fructueux ont été menés à bien. On peut se demander si les deux pistes de travail qui ont été suivies correspondent à deux étapes ou à deux époques.

1. - La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel a été adoptée le 28 janvier 1981 (STCE n° 108). Les travaux préparatoires ont été menés dans le cadre du Comité directeur de la coopération juridique (CDCJ), par un comité ad hoc (CAHIL) et non dans celui du Comité directeur des droits de l'homme (CDDH), introduisant ainsi une nouvelle césure dans le système de protection des droits de l'homme, après la Charte sociale européenne, ce qui n'est pas sans conséquence. Le choix d'un instrument spécialisé, fonctionnant comme une convention-cadre complétée par des protocoles et des résolutions, écarte tout rattachement direct ou indirect à la Cour européenne des droits de l'homme. Néanmoins le préambule de la Convention était sans ambiguïté en « *considérant qu'il est souhaitable d'étendre la protection des droits de l'homme de chacun, notamment le droit au respect de la vie privée, eu égard à l'intensification de la circulation à travers les frontières des données à caractère personnel faisant l'objet de traitements automatisés* », tout en « *réaffirmant en même temps leur engagement en faveur de la liberté d'information sans considération de frontières* ». Le préambule soulignait ainsi « *la nécessité de concilier les valeurs fondamentales du respect de la vie privée et de la libre circulation de l'information entre les peuples* »[11].

Significativement, le titre de la convention ne comporte pas de référence européenne - contrairement à la pratique habituelle des « conventions européennes » conclues sous

[10] HRI/GEN/I/Rev.8.
[11] *Cf.* le site du bureau des traités du Conseil de l'Europe, http://conventions.coe.int.

les auspices du Conseil de l'Europe - pour souligner son caractère de « traité ouvert », mais en pratique cette clause n'a pas eu l'effet escompté, tandis que les amendements de 1999 permettant l'adhésion des Communautés européennes ne sont pas encore entrés en vigueur. Avec 38 ratifications et 4 signatures (Moldova, Russie, Turquie, Ukraine) la convention lie la plupart des Etats membres du Conseil de l'Europe. Un protocole additionnel (STCE n° 181) concernant les autorités de contrôle et les flux transfrontières de données a été adopté le 8 novembre 2001. Au 1er janvier 2007, il comportait 13 Etats parties et 17 signataires (dont la France et le Royaume-Uni). Mais malgré le succès quantitatif de la convention de 1981, le système – faute d'être ancré dans les droits de l'homme – reste fragile. D'autant que le régime protecteur établi au sein du Conseil de l'Europe se trouve concurrencé, voire remis en cause dans le cadre de l'Union européenne, dans une toute autre logique, plus commerciale, influencée par les groupes d'intérêts privés.

2. - La montée en puissance du droit communautaire s'est traduite non sans mal par l'adoption de la directive 95/46/CE 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. Le glissement du titre est symptomatique : le libéralisme économique l'emporte sur l'individualisme libéral. D'autres textes ont été adoptés ou sont en gestation, à la suite de la directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications (dénommée directive « vie privée et communications électroniques ») qui remplaçait elle-même la directive 97/66/CE du 15 décembre 1997 du même nom.

La mise en place de ce cadre européen a entraîné une adaptation des différentes législations nationales. Sans entrer dans les détails, on peut noter que la Commission nationale informatique et libertés comme la Commission nationale consultative des droits de l'homme ont suivi avec beaucoup de vigilance cette évolution sans doute inéluctable qui marquait une érosion des certitudes sur les quelles étaient fondées la loi de 1978 et la convention de 1981. On peut se référer notamment aux avis de la CNCDH du 22 septembre 1994 et du 21 mars 1995 sur la directive européenne relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel, et plus récemment dans un cadre plus large à la note du président de la CNCDH du 15 décembre 2005 « sur le projet de loi relatif à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers », à une étude - qui est prudemment appelée une « contribution de la CNCDH au débat » - adoptée le 1er juin 2006 sur les « problèmes posés par l'inclusion d'éléments biométriques dans la carte nationale d'identité »[12]. Mais ces travaux récents s'inscrivent dans un nouveau contexte, celui de la remise en cause du système de protection.

[12] *Cf.* le site de la CNCDH, www.cncdh.fr.

II. – LA REMISE EN CAUSE DU SYSTEME DE PROTECTION

Dans un monde « globalisé » rendu instantané par les nouvelles technologies, les protections juridiques traditionnelles, qu'elles soient nationales ou même européennes, sont vaines face au risque de paradis cybernétiques immatériels plus que délocalisés, comme pouvaient l'être les « radios pirates ». On l'a vu dans le domaine classique de la liberté de l'information, s'agissant de la protection de la vie privée, du secret médical ou de la censure, c'est encore plus vrai pour la protection des données personnelles. Mais cette révolution technique va de pair avec une crise politique.

1. - La coopération pénale internationale, dominée par la lutte contre le terrorisme ou la corruption, implique d'une part une surveillance accrue des mouvements suspects - transports aériens, mouvements de fonds - mais aussi des transferts de données à l'échelle internationale. Cette évolution implique une série de menaces pour les libertés publiques : d'abord l'interconnexion des fichiers autorisés, au nom d'une efficacité plus grande, alors que le cloisonnement était un principe de protection et de vérification ; ensuite les transferts internationaux de données sans garanties équivalentes, enfin les risques nés de l'implication plus ou moins clandestine des acteurs privés (compagnies aériennes, banques).

Sur le terrain juridique la question des relations entre l'Union européenne et les Etats-Unis se posait dans des termes difficiles, avant même de 11 septembre et la « guerre contre le terrorisme ». La directive de 1995 remettait en cause la protection nationale des données en autorisant des transferts en cas de protection équivalente dans le pays destinataire. Les mises en garde du Parlement européen n'ont pas empêché la Commission européenne de négocier un accord bilatéral avec les Etats-Unis estimant que ce pays offrait des garanties équivalentes. Dès 1999, la Commission a mis au point un accord avec les Etats-Unis sur le niveau de protection assuré par les principes de la sphère de sécurité (*safe harbour*) qui a débouché sur une décision de principe du 26 juillet 2000. Ce qui était sans doute déjà discutable à l'époque me semble l'être encore plus à la suite du *Patriot Act* et des autres mesures prises par l'administration républicaine. Après des négociations difficiles, nouvel accord a été conclu le 28 mai 2004 « sur le traitement et le transfert des données PNR par des transporteurs aériens au bureau des douanes et de la protection des frontières du ministère américain de la sécurité intérieure ». Saisie par le Parlement européen, la CJCE a, par son arrêt du 20 mai 2003, remis en cause la base juridique de l'accord, sans se pencher sur le fond, et notamment son caractère discriminatoire et attentatoire à la vie privée[13]. La Commission s'est empressée de conclure un accord identique, sur une nouvelle base, signé à Washington le 19 octobre 2006.

[13] *Cf.* le dossier *Data Protection* sur le site Justice affaires intérieures (JAI) de la Commission européenne, http://ec.europa.eu/justice_home/index_en.htm.

Le préambule de l'accord de 2006 entre l'Union européenne et les Etats-Unis montre bien le déplacement du point d'équilibre qu'avait cherché à établir la convention de 1981. Les deux parties « *reconnaiss[e]nt qu'il importe de prévenir et de combattre le terrorisme et les délits qui y sont liés, ainsi que d'autres délits graves de nature transnationale, y compris la criminalité organisée, tout en respectant les droits et libertés fondamentales et notamment le droit au respect de la vie privée* ». Mais en dehors d'un visa de « *l'article 6, paragraphe 2, du traité de l'Union européenne concernant le respect des droits fondamentaux, et notamment le droit à la protection des données à caractère personnel qui s'y rattache* », le contenu de l'accord comporte peu de garanties.

Il est seulement précisé que le *Department of Homeland Security (DHS)* traitera « *les données PNR reçues et les personnes concernées par ce traitement conformément aux lois et exigences constitutionnelles américaines applicables, sans discrimination illégitime, en particulier sur la base de la nationalité et du pays de résidence* » (§ 3). Cette vague garantie peut sembler n'être qu'une pétition de principe, dans la mesure où « *aux fins de l'application du présent accord, le DHS est réputé assurer un niveau adéquat de protection des données PNR transférées de l'Union européenne concernant un service international de passagers à destination ou au départ des Etats-Unis* » (§ 6). Pour le reste l'Union européenne pourra invoquer à son bénéfice « *le strict respect du principe de réciprocité* » (§ 5), tandis que l'accord bilatéral ne constitue pas un précédent pour d'autres négociations entre les deux parties ou avec des tiers « *au sujet du traitement et du transfert de données PNR ou de toute autre forme de données* », même si assez curieusement « *s'appuyant sur le présent accord, l'UE confirme qu'elle ne fera pas obstacle au transfert de données PNR entre le Canada et les Etats-Unis et que le même principe s'appliquera à tout accord similaire concernant le traitement et le transfert de données PNR* ». Autrement dit, si l'Union européenne étend l'accord bilatéral au Canada qui constitue un partenaire naturel, elle signe également un chèque en blanc aux Etats-Unis pour toute sous-traitance des données à n'importe quel pays tiers … y compris un partenaire n'offrant pas les garanties juridictionnelles d'un Etat de droit. De transfert en transfert, on risque de s'éloigner de la notion de « sphère de sécurité », de « *safe harbour* » pour sombrer dans le non-droit des paradis informatiques.

2. - Mais les Etats ne sont pas ou plus les seuls à faire peser des menaces sur le système de protection mis en place depuis trente ans. Certes, dès le début, les sociétés de vente par correspondance avaient fait à Strasbourg et à Bruxelles un lobby important pour constituer des fichiers détaillés des clientèles potentielles. Avec l'essor d'Internet, le problème a pris une toute autre dimension et paraît hors de contrôle. Le groupe d'experts indépendants en matière de droits fondamentaux – établi auprès de la direction justice affaires intérieures de M. Frattini – a d'ailleurs adopté un avis n° 4 le 1er décembre 2003 sur la protection de l'internaute au regard de ses données à caractère personnel, s'agissant notamment des atteintes aux droits de propriété intellectuelle[14]. Est en jeu également la conservation des données des communications électroniques à des fins d'enquêtes criminelles, avec la directive communautaire 2006/24/CE relative à la conservation des

[14] CFR-CDF avis 4-2003.

données adoptée par le Parlement européen et la Commission le 15 mars 2006[15] et sa transposition en France par le décret du 24 mars 2006 qui fixe un délai de conservation d'une année[16]. A ce stade la menace reste diffuse mais ce n'est pas un hasard si le thème de la dernière réunion des instances de protection des données, tenue à Londres à l'automne dernier, a porté sur l'avènement d'une « *société de surveillance* ». C'est également l'objet de récentes mises en garde de l'*Information Commissioner*, Richard Thomas[17].

Au-delà des craintes ponctuelles liées à la vidéosurveillance, c'est une société caractérisée par la traçabilité de tous les faits et gestes de chaque individu (portables, cartes à puces, mémoire des ordinateurs) qui menace notre conception traditionnelle de la vie privée. Face à ce fantasme totalitaire ou à une liberté absolue tout aussi menaçante, on doit se demander si le régime de contrôle des données personnelles fondé sur l'intervention d'autorités administratives indépendantes, patiemment mis en place depuis 30 ans, constitue un combat d'avant-garde ou une ligne Maginot, condamnée à être dépassée par la révolution des nouvelles technologies ?

Sans répondre à cette question, il est certain que la solution ne pourra être trouvée ni dans l'autarcie nationale, ni même dans le cadre régional, mais à l'échelle mondiale. A l'ère de la mondialisation omniprésente et de la transparence absolue, comment réinventer le respect de la « *privacy* », le sens de l'intimité, l'espace de liberté qui constitue le for intérieur de chacun de nous, ou ce qu'André Malraux appelait « *ce misérable petit tas de secrets* » ? Aurions-nous sacrifié la liberté des modernes, le mur de la vie privée, tout en abdiquant la liberté des anciens, celle de l'espace démocratique ?

[15] JO L 105 du 13 avril 2006, p. 54.
[16] *Cf.* le point de vue du responsable de la protection des données personnelles pour Google Europe, Peter FLEISCHER, « La protection de la vie privée sur Internet », *Le Monde*, 6 avril 2007.
[17] *The Observer*, 29 avril 2007.