LES ENTREPRISES FACE À LA PROTECTION DES DONNÉES PERSONNELLES : CONTRAINTES SUBIES ET RESPONSABILITÉS CROISSANTES

par
Bertrand WARUSFEL

(publié in *Revue Française d'Administration Publique*,
janvier-mars 1999, n° 89, pp. 105-117)

La loi du 6 janvier 1978 a institué un dispositif juridique garantissant les libertés des personnes physiques à l'occasion des traitements informatiques et les protégeant plus particulièrement à l'encontre des traitements effectués par des personnes publiques ou appartenant au secteur public. Autant dire que l'entreprise, en tant qu'acteur économique et que personne morale de droit privé à but lucratif n'a pas été au coeur des préoccupations du législateur de 1978. Pourtant avec un recul de vingt années et à l'heure de la transposition de la directive européenne de 1995, force est de constater que ce sont aujourd'hui ces mêmes entreprises qui sont les principaux *"maîtres de fichiers"* et donc les premières concernées par l'application de cette loi.

S'il est donc incontestable que la protection des données nominatives s'impose pleinement aux entreprises privées **(I)**, celles-ci éprouvent souvent certaines difficultés à mettre en oeuvre les dispositions de la loi de 1978 et à les concilier avec les autres dimensions de leurs activités économiques **(II)**. Mais les évolutions en cours du cadre juridique européen tout comme des technologies de communication aujourd'hui disponibles replacent ces questions sous un jour nouveau et impose de confier aux entreprises une plus grande responsabilité dans la protection des données personnelles **(III)**.

I. Des entreprises soumises aux obligations de protection des données personnelles

La lecture de la loi du 6 janvier 1978 fait apparaître clairement à plusieurs reprises le fait que les entreprises privées sont explicitement visées par ses dispositions (1.), mais il n'en demeure pas moins qu'elle consacre une différence de traitement entre secteur public et secteur privé, en faveur de ce dernier (2.). Mais la contrepartie en est que les données d'entreprise ne sont pas protégées, en tant que telles, par la loi (3.).

1.1. Les entreprises sont concernées par l'application de la loi

Plusieurs dispositions de la loi du 6 janvier 1978 font explicitement référence aux entreprises privées et aux traitements qu'elles peuvent réaliser en matière de données nominatives, auxquelles elles ont vocation à s'appliquer intégralement.

L'article 2 met ainsi sur le même pied toute *"décision administrative ou privée"* et l'article 14 parle indifféremment des traitements automatisés qu'ils soient *"publics ou privés"*. Plus loin encore, le dernier alinéa de l'article 21 précise que *"les ... dirigeants d'entreprises, publiques ou privées, responsables de groupements divers et plus*

généralement les détenteurs ou utilisateurs de fichiers nominatifs ne peuvent s'opposer à l'action de la commission".

Enfin, depuis l'entrée en vigueur du nouveau code Pénal, l'article 226-24 nCP prévoit spécifiquement la responsabilité pénale des personnes morales en cas d'infraction aux dispositions relatives aux données nominatives.

L'applicabilité des dispositions de la loi de 1978 aux traitements mis en oeuvre par des entreprises du secteur privé ne fait donc aucun doute. Et il en ira de même lorsque s'appliqueront les dispositions issues 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. Cette directive désigne, en effet, en tant que responsable du traitement *"la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel"* et son considérant 25 précise explicitement que *"les principes de la protection doivent trouver leur expression, ..., dans les obligations mises à la charge des personnes, autorités publiques, entreprises, agences ou autres organismes qui traitent des données..."*.

1.2. Des procédures administratives jusqu'à présent distinctes de celles applicables au secteur public

Mais si les entreprises privées sont soumises au respect des dispositions de la loi de 1978, tout comme les services publics ou les personnes physiques, il faut cependant relever que cette loi a voulu appliquer au secteur public un régime juridique plus rigoureux que celui réservé au secteur privé.

Cette distinction public-privé ressort clairement de la lecture de l'article 15 de la loi qui soumet la création de tout traitement informatisé à l'obligation de l'adoption d'un acte réglementaire, pris après avis motivé de la Commission nationale de l'informatique et des libertés (CNIL), dès lors que ces traitements sont *"opérés pour le compte de l'Etat, d'un établissement public ou d'une collectivité territoriale, ou d'une personne morale de droit privé gérant un service public"*.

A l'inverse, et sans plus de précision quant au statut juridique des entités concernées, l'article 16 indique que les traitements effectués *"pour le compte de personnes autres que celles soumises aux dispositions de l'article 15"* ne sont soumis qu'à la seule formalité de la déclaration préalable. C'est donc cette dernière qui s'applique le plus généralement lors de la création par une entreprise privée d'un traitement de données nominatives, la seule exception étant celle des entreprises délégataires d'une mission de service public.

Ainsi donc, si les entreprises privées sont bien concernées par l'application de la loi de 1978 et les règles protégeant les données nominatives, elles bénéficient, le plus souvent, d'un régime juridique allégé, qui les dispensent de devoir attendre l'écoulement d'un délai d'examen (2 mois renouvelables, en cas de demande d'avis) avant de pouvoir mettre en oeuvre le traitement et les met à l'abri d'un possible (bien

que très rare) avis défavorable. Allant plus loin encore, la CNIL a usé largement du pouvoir que lui donnait l'article 17 de la loi de 1978 pour établir des *"normes simplifiées"* permettant d'alléger les procédures pour la déclaration des *"catégories les plus courantes de traitement à caractère public ou privé"* et dont plus de la moitié d'entre elles couvrent actuellement les aspects les plus récurrents de l'utilisation de l'informatique dans l'entreprise. [1]

Cette inégalité de traitement entre les entreprises et le secteur public est l'un des aspects qui doit disparaître avec la transposition prochaine en droit français de la directive du 24 octobre 1995 qui se caractérise, justement, par *"l'égalité de principe entre secteur public et privé"* [2]. Mais cette discrimination aura marqué les deux premières décennies de protection des données personnelles en France et, indirectement, aidé à faire en sorte que les entreprises acceptent de se soumettre aux obligations d'une législation qui ne leur procure aucun avantage propre.

1.3. Une protection qui ne couvre pas, en tant que telles, les données d'entreprise

Cette apparente facilité de procédure reconnue aux personnes morales de droit privé a son revers, en ce sens que les entreprises - même soumises à des obligations administratives allégées - ne tirent que très indirectement profit de l'application des dispositions protégeant les données nominatives. En effet, même si la convention du 28 janvier 1981 du Conseil de l'Europe prévoit la possibilité pour les Etats membres d'étendre la protection relative aux données personnelles *"à des informations afférentes à des groupements, associations, fondations, sociétés, corporations ou à tout autre organisme regroupant directement ou indirectement des personnes physiques et jouissant de la personnalité juridique"* [3], la loi française actuelle ne prévoit aucune disposition particulière permettant à une entreprise de revendiquer sur des informations la concernant en tant que telle, les droits par ailleurs reconnus aux personnes physiques. Et il en va de même s'agissant de la directive de 1995.

Tout au plus, la CNIL a-t-elle reconnu - s'agissant de *"personnes physiques, représentants légaux des entreprises"* - que *"dès lors que le nom de ces personnes figure dans le fichier en tant que dirigeant, actionnaire ou associé"*, celles-ci peuvent faire valoir leur droit d'accès [4]. Mais dans cette même délibération relative à des fichiers de personnes morales mises en oeuvre par les communes, la Commission a bien expressément rappelé que *"le droit d'accès établi par l'article 34 de la loi du 6 janvier 1978 a un caractère strictement individuel"* , soulignant ainsi indirectement que - même dans le cas où le fichier regroupe des données sur des entreprises - l'entreprise ne reçoit pas de droit d'accès propre et concernant l'ensemble des

[1] Par exemple, les fichiers de paie (norme simplifiée n° 28), les fichiers clients (norme simplifiée n° 11), les fichiers fournisseurs (norme simplifiée n° 14) ou encore les fichiers d'adresses utilisées pour des "mailing" (norme simplifiée n° 15).
[2] Guy Braibant, Données personnelles et société de l'information - Transposition en droit français de la directive 95/46 - Rapport au Premier ministre, La documentation française, 1998, p. 60.
[3] Article 3.2.b Convention du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement des données à caractère personnel.
[4] Délibération 84-28 du 3 juillet 1984, reproduite in CNIL, *5ème rapport* , p. 254.

données qui la concernent, mais que seuls les représentants de la société peuvent agir sur la base et dans la limite de leurs seuls droits individuels [5].

Dans le même sens d'une dissymétrie entre les droits des personnes physiques et ceux des personnes morales, le commissaire du gouvernement Combrexelle faisait justement remarquer dans des conclusions de 1997 qu'"il n'y a pas (en revanche), une liberté constitutionnelle de mettre en oeuvre un fichier automatisé. Certes la liberté d'entreprendre est également en cause lorsque le traitement automatisé est exploité par une entreprise. Mais outre que cette liberté ne concerne pas toutes les personnes privées, le législateur n'a pas voulu, ainsi que cela ressort des travaux préparatoires, placer cette liberté sur le même plan que les libertés individuelles protégées par la loi" [6].

Au total, si l'entreprise est bien concernée par l'application de la loi de 1978, elle jouit dans ce dispositif d'un statut subalterne qui, s'il lui permet de bénéficier de contraintes allégées (tout au moins en comparaison de celles imposées aux personnes publiques), ne lui donne aucun droit particulier et ne lui procure aucun moyen nouveau de protéger juridiquement les informations qui la concernent. Dans ces conditions, il faut donc reconnaître, en pratique, que les entreprises ont souvent éprouvé des difficultés à mettre en oeuvre les dispositions de la loi de 1978 et à les concilier avec les impératifs de la vie des affaires.

II. Une protection jusqu'à présent difficile à intégrer dans la pratique des entreprises

Contrepartie sans doute de l'application d'un régime formellement libéral et dont les buts (la protection de la vie privée) ne sont pas en rapport direct avec la finalité des activités économiques, on peut notamment relever deux types de difficultés qu'éprouvent les entreprises à se plier effectivement aux obligations de la loi Informatique et Libertés. La première difficulté réside dans l'insécurité juridique dans laquelle la procédure déclarative les contraint de demeurer (1.) tandis que, plus profondément, les entreprises sont pas toujours en mesure d'intégrer les contraintes de la protection des données personnelles dans le cadre général de leurs obligations juridiques (2.).

2.1. Les incertitudes juridiques de la procédure déclarative

Les traitements d'informations nominatives effectués par des entreprises du secteur privé relèvent tous actuellement de la procédure déclarative (éventuellement réduite, en cas de référence à une norme simplifiée), laquelle doit prochainement devenir la procédure de droit commun pour tout les traitements, même publics, à l'exception de ceux "susceptibles de présenter des risques particuliers au regard des droits et

[5] La personne morale peut, tout au plus, invoquer les dispositions de droit commun pour obtenir la rectification d'informations erronées la concernant (cf. TGI Paris 24 avril 1984, Galande).
[6] Jean-Denis Combrexelle, conclusions sous CE, 6 janvier 1997, Caisse d'épargne Rhône Alpes Lyon, *RFDA*, mai-juin 1997, p. 555.

libertés des personnes concernées" (article 20 de la directive 95/46) qui resteront soumis à un examen préalable.

Mais cette procédure déclarative - plus légère à mettre en œuvre que la procédure de demande d'avis - entraîne des conséquences juridiques qui n'ont pas toujours été bien comprises et bien acceptées par le monde des entreprises privées.

L'article 16 de la loi précise, en effet, que "cette déclaration comporte l'engagement que le traitement satisfait aux exigences de la loi. Dès qu'il a reçu le récépissé délivré sans délai par la commission, le demandeur peut mettre en oeuvre le traitement. Il n'est exonéré d'aucune de ses responsabilités".

L'interprétation de ce texte, tant par les entreprises déclarantes que par la CNIL elle-même, a pu donner lieu à certaines difficultés, voire à certains malentendus, concernant notamment les pouvoirs d'instruction de la Commission face aux dossiers déclaratifs.

La CNIL avait pris l'habitude de considérer que la loi mentionnant explicitement l'engagement de conformité du traitement, elle avait le droit et le devoir d'effectuer une première vérification du contenu de la déclaration et dans le cas où il s'avérait que celle-ci comportait des éléments manifestement contraires aux dispositions de la loi, de refuser la délivrance du récépissé de déclaration. Ainsi, dans une délibération de décembre 1995, la Commission - après avoir pris connaissance d'une déclaration de modification d'un traitement - statuait dans ces termes : "en conséquence, est d'avis, les conditions de la mise en oeuvre du traitement n'étant pas conformes aux dispositions de la convention n°108 du Conseil de l'Europe et à celles de la loi du 6 janvier 1978, qu'en l'état, le récépissé de la déclaration de modification ne peut être délivré" [7].

Cette interprétation extensive des pouvoirs de la CNIL dans le cadre de la procédure déclarative a été logiquement censurée par le Conseil d'Etat dans un arrêt du 6 janvier 1997. Appliquant à cette matière la logique qui avait amené les tribunaux administratifs à affirmer la compétence liée de l'autorité administrative en matière de délivrance du récépissé de déclaration des associations [8], la Haute juridiction a considéré que le rôle de la CNIL doit se limiter à vérifier l'existence des précisions exigées par l'article 19 de la loi (qui fixe le contenu des renseignements à fournir dans le dossier de déclaration) et de l'engagement de conformité prévu à l'article 16, sans aller jusqu'à vérifier au fond ladite conformité du traitement, et - sur ce fondement - a annulé le refus de délivrance du récépissé, qui avait été opposé par la CNIL à une Caisse d'épargne au motif que le mode de collecte et les conditions d'exercice du droit d'opposition ne lui paraissaient pas satisfaisants [9].

Si l'on se place du point de vue de l'entreprise déclarante, on est tenté de considérer, en première analyse, qu'en rappelant ainsi à la CNIL les strictes limites que lui impose la procédure déclarative, le Conseil d'État a réaffirmé les droits des

---

[7] Délibération n° 95-162 du 19 décembre 1995, reproduit in CNIL, *16ème rapport d'activité 1995*, La documentation Française, 1996, p. 128.
[8] Cf. notamment TA Paris, 25 janvier 1971, Simone de Beauvoir, M. Leyris.
[9] CE, 6 janvier 1997, Caisse d'épargne Rhône Alpes Lyon, *RFDA*, mai-juin 1997, p. 558.

entreprises privées, sur lesquels empiétait indiscutablement la pratique de cette respectable autorité administrative. Mais, à mieux y regarder, il n'est pas sûr que cette clarification n'ait pas contribué à accroître l'insécurité juridique que ressentent fréquemment les entreprises face aux obligations de la loi de 1978.

En effet, la plupart des entreprises utilisatrices de systèmes informatiques souhaiteraient pouvoir, par une démarche administrative unique et définitive, s'assurer de la licéité de leur traitement et ainsi s'exonérer, par avance, de toute forme de mise en cause ultérieure de leur responsabilité. Or ce désir de recevoir - en quelque sorte - un certificat de conformité va directement à l'encontre de la lettre de l'article 16 précité qui rappelle que, même lorsqu'il est en possession du récépissé délivré par la CNIL, le déclarant "n'est exonéré d'aucune de ses responsabilités". C'est pourquoi, paradoxalement, la pratique litigieuse de la CNIL exerçant une certaine forme de contrôle préalable sur la licéité du traitement déclaré était, somme toute, relativement acceptée par les entreprises qui, dès lors que le récépissé leur était délivré, s'estimaient implicitement validées par la CNIL [10]. Le retour à une application plus respectueuse du texte original replace donc, à l'inverse, les entreprises déclarantes devant une incertitude juridique latente dont la plupart ne sont pas en état d'assumer les conséquences.

C'est peut-être, d'ailleurs, la raison pour laquelle, quelques mois seulement après son arrêt de janvier 1997, le Conseil d'État assortit sa position d'une précision qui n'était pas sans importance. Statuant sur les suites de la même délibération de décembre 1995 précitée, après que la CNIL eut entre-temps délivré le récépissé primitivement refusé, la Haute assemblée considéra que c'était à bon droit que la CNIL avait cependant adressé un avertissement à la société déclarante [11]. En d'autres termes, si la Commission ne peut - en refusant de délivrer le récépissé - transformer une procédure de déclaration en une procédure d'autorisation déguisée, elle conserve le droit de faire connaître officiellement au déclarant ses réserves sur la conformité de son traitement aux dispositions légales en vigueur.

Toute cette problématique paradoxale devrait vraisemblablement perdurer - voire s'accentuer - sous l'empire des dispositions issues de la directive 95/46. En effet, l'une des particularités de ce texte est, en élargissant considérablement le champ des procédures de notification et en restreignant les cas de recours à un examen préalable, d'effectuer - comme l'indique M. Braibant - "un glissement d'un contrôle a priori vers un contrôle a posteriori" [12].

---

[10] L'existence - en marge des dispositions de la loi elle-même - de pratiques indirectes conciliantes a souvent caractérisé l'attitude de la CNIL vis-à-vis des entreprises. Ainsi, témoignant dans une affaire contentieuse, le représentant de la CNIL n'hésita pas à reconnaître que "le défaut de déclaration avant l'exploitation de fichiers se réglait quasiment toujours à l'amiable, l'intéressé étant invité par la CNIL à régulariser sa situation" (Procureur de la République c./ Jean-Baptiste B. et Jean-Michel D., TGI Paris, 17ème chambre, 17 octobre 1994).

[11] "[considérant] ... que, dans les circonstances de l'espèce, la CNIL a pu sans commettre d'erreur de droit ni d'erreur d'appréciation estimer que le nouveau traitement ne présentait pas des garanties suffisantes pour permettre aux personnes interrogées d'exercer le droit d'opposition qui leur est reconnu par l'article 26 précité ; que, par suite, la Commission a pu légalement adresser pour ce motif un avertissement à la Société Consodata" (CE, 30 juillet 1997, Sté Consodata, reproduit in CNIL, *18ème rapport d'activité 1997*, La documentation Française, 1998, p. 384).

[12] G. Braibant, op. cit., p. 61.

2.2. Des contraintes spécifiques qui ne s'intègrent qu'imparfaitement dans les catégories du droit de l'entreprise

Soucieuses avant tout de l'efficacité et de la performance de leur gestion, les entreprises expriment toujours le souhait que le législateur ne leur créé pas de nouvelles contraintes administratives ou juridiques qui soient sans rapport logique et direct avec leurs activités économiques. C'est pourquoi, les obligations nées de la loi du 6 janvier 1978 ont souvent été perçues, dans le secteur privé, comme étant un dispositif juridique hétérogène difficile à resituer dans l'ensemble du droit de l'entreprise.

Si l'on accepte, un moment, de sacrifier à une interrogation théorique, à quelle grande dimension du droit de l'entreprise, ces dispositions pourraient-elles, en effet, se raccrocher ? Dans la mesure où elles sont - pour l'essentiel - relatives au traitement informatique des données et où l'informatisation des entreprises est aujourd'hui une réalité quasi-générale, la facilité voudrait qu'elles puissent s'intégrer harmonieusement aux autres aspects juridiques liés à l'usage de l'informatique dans l'entreprise. Mais, malheureusement, ce domaine de l'informatique demeure particulièrement rétif (sans doute, parce qu'il est encore récent et en trop grande évolution) à toute systématisation. Si l'on parle, par commodité, d'un "droit de l'informatique", il ne s'agit, en réalité, encore que d'une mosaïque de dispositions sans unité. Entre les dispositions sur le droit d'auteur applicable à certaines créations informatiques (logiciels et certaines bases de données), celles pouvant protéger, de façon *sui generis*, certains producteurs de base de données [13], ou celles qui répriment des actes de fraude informatique, la loi de 1978 ne fait qu'ajouter à un inventaire qui reflète surtout la répugnance (consciente ou inconsciente) de notre tradition juridique française à créer un droit spécifique propre au support informatique. De plus, la nature même des données visées par les textes relatifs à la protection des données personnelles ne recouvre qu'une partie de l'"ensemble des données informatiques qu'une entreprise peut avoir à traiter dans son système d'information". D'où il résulte que l'application d'un dispositif comme celui de la loi du 6 janvier 1978 conduit les entreprises à devoir faire une distinction purement juridique entre des traitements techniquement semblables, sur le seul fondement du caractère nominatif possible des données traitées.

A défaut donc de s'intégrer dans un droit de l'informatique encore à créer (et qui serait un droit du support, un droit du "contenant"), les règles applicables aux données personnelles pourraient-elles se rattacher à un quelconque droit du "contenu" ? Ce serait intellectuellement satisfaisant, tant il est vrai que c'est à raison de leur contenu (directement ou indirectement nominatif) que certaines données relèvent de l'application de la loi du 6 janvier 1978. Mais là encore, la réalité est peu encourageante. Le seul élément cohérent et stable d'un droit des contenus dans la sphère économique et commerciale est constitué par la propriété intellectuelle dans ses différentes branches (propriété littéraire et artistique, droits de propriété industrielle). Mais, à l'évidence (et quelles que soient les tentations théoriques de

[13] Cf. les articles L 341-1 à 343-4 du Code de la propriété intellectuelle, introduits par la loi du 1er juillet 1998.

certains pour plaider en faveur d'un droit de propriété sur les données personnelles [14]), les droits et obligations que la loi de 1978 fait peser sur les données nominatives ne se rattachent à aucune forme d'appropriation patrimoniale et ne peuvent se rattacher (et, encore, que de manière partielle) qu'à la catégorie quelque peu imprécise des "droits de la personnalité" [15]. Or, au-delà du champ bien balisé de la propriété intellectuelle, les autres éléments d'un éventuel "droit de l'information" composent un agrégat fort hétéroclite : outre les droits de la personnalité (droit à l'image, droit au nom, droit au respect de la vie privée, ..) déjà évoqués, on peut évoquer les règles très disparates applicables à la protection de certains secrets (secret de défense, secret professionnel, secret de fabrique, ...) ou encore celles réprimant certains usages d'informations (délit d'initié, propagation de fausses nouvelles, diffamation, ...). A côté de tout cela, la réglementation de l'usage des données personnelles a bien une place, mais cela ne fournit pas à l'entreprise commerciale un cadre juridique clair lui permettant de gérer commodément ce type de contraintes.

En élargissant encore la perspective, il serait tentant de vouloir restituer la protection des données personnelles dans le cadre vaste et englobant du droit commercial, qui régit l'ensemble des relations existant entre l'entreprise et ses clients ou fournisseurs. Mais, à nouveau, la tentative parait vouée à l'échec, car il apparaît tout de suite que la problématique de l'usage des données personnelles dans l'entreprise ne se réduit pas à des pratiques commerciales. En effet, tout autant que les données de clientèle, les données sociales relatives aux salariés de l'entreprise relèvent naturellement de l'application de la loi de 1978. Et, plus profondément, il est clair que les ressorts profonds de la réglementation des données personnelles échappent complètement à la logique qui anime le droit des affaires et se rattachent à d'autres dimensions du droit (droit des personnes et libertés publiques, principalement).

Il faut donc constater que les règles relatives aux données personnelles dont la loi impose le respect aux entreprises, ne trouvent pas leur place dans les différentes catégories traditionnelles du droit de l'entreprise. Et cela ne soulève pas seulement une difficulté théorique mais débouche aussi indirectement sur une réalité pratique : ne sachant pas où et comment rattacher cette contrainte exogène dans leur organisation juridique et leurs procédures internes, beaucoup d'entreprises prennent le risque de ne pas se mettre ou demeurer en conformité avec les différentes exigences de la loi en cette matière.

III. Vers une meilleure prise en compte du rôle des entreprises dans la protection des données personnelles ?

Deux évolutions majeures vont renouveler les conditions de la protection des données personnelles dans les prochaines années. Une de ces évolutions est technico-économique : il s'agit du développement massif de la communication et du

[14] Pour une critique de ces théories, cf. Nathalie Mallet-Poujol, "Appropriation de l'information : l'éternelle chimère", Dalloz, 1997, pp. 330-336.

[15] De plus, à supposer qu'une quelconque appropriation puisse s'appliquer à ces données, elle ne jouerait qu'au profit des personnes physiques concernées, ce qui ne réglerait pas réellement la situation des entreprises dépositaires de ces données, auxquelles il faudrait attribuer une forme particulière de droit d'exploitation.

commerce électronique. L'autre facteur est juridique, puisqu'il s'agit de la transposition et de l'entrée en vigueur en Europe des dispositions de la directive de 1995. Dans quelle mesure, ces deux phénomènes parallèles peuvent-ils modifier la manière dont les entreprises seront prises en compte et dont elles assumeront la lourde responsabilité de veiller à l'usage des données personnelles qu'elles exploitent ?

3.1. Un rôle croissant des entreprises dans l'exploitation et la protection des données

Toutes les analyses convergent pour admettre que le développement de l'Internet et des nouvelles formes de commerce sur les réseaux de communication électronique va faire des entreprises privées les principaux exploitants de données personnelles à l'échelle mondiale.

Cela provient, d'abord, du fait que les moyens électroniques favorisent considérablement l'identification directe ou indirecte des personnes. Cela est vrai à l'intérieur des entreprises elles-mêmes au sein desquelles l'usage croissant des réseaux locaux et de l'Intranet, associés à d'autres moyens électroniques (tels les standards téléphoniques numériques, les téléphones mobiles ou les systèmes de contrôle d'accès par badge) donne aux employeurs des possibilités croissantes d'acquisition et d'exploitation de données personnelles relatives à leurs salariés.

Mais cela va être de plus en plus le cas également dans les relations entre les entreprises et leurs clients ("business to client") ou entre les entreprises elles-mêmes ("business to business"). Il faut noter, en effet, que tant les nécessités de sécurité qu'implique le commerce électronique (identification des parties à la transaction, signature des échanges, exigence de non-répudiation ...) que les besoins de protéger la propriété intellectuelle des créations numériques (contre le piratage et la contrefaçon en ligne) poussent les entreprises et les consommateurs à recourir à des moyens d'authentification de plus en plus performants [16]. Le paradoxe en devient, de ce fait, extrême : plus les entreprises et leurs clients recherchent une sécurisation de leurs échanges, plus la collecte de données personnelles s'intensifie et s'automatise !

Mais, une fois ces données collectées par les serveurs électroniques des entreprises, le phénomène s'accroît encore par le fait que - comme le souligne le rapport Braibant - de "nombreux opérateurs économiques fondent aujourd'hui l'essentiel de leur activité sur le traitement et le transfert d'informations nominatives" [17]. En effet, toutes les activités liées au commerce et aux prestations de service (banque, assurance, services de réservation [18], services d'information, ...)

[16] Ce besoin d'authentification fut à l'origine de la première tentative d'assouplissement de la réglementation française de la cryptologie en 1996-1998, qui visait - tout en maintenant un contrôle strict sur les moyens de chiffrement - à rendre libre l'usage des moyens d'authentification et de signature destinés au commerce électronique (cf. notamment Bertrand Warusfel, "Le régime juridique de la cryptologie en France : opportunités et limites de la nouvelle réglementation", Droit & Défense, 98/1 p.66).

[17] Cf. G. Braibant, op. cit., p. 13.

[18] Sur les services de réservation aérienne et les difficultés qu'ils présentent au regard de la protection des données personnelles, cf. Isabelle Jaulin, "Le village global : Enjeux et problèmes - Les systèmes interactifs internationaux de réservation et la protection des données personnelles", Intervention à la 18ème Conférence internationale Protection de la vie privée et des données nominatives, Ottawa, 18-20 septembre 1996.

vont tirer l'essentiel de leur valeur ajoutée de l'exploitation et de l'enrichissement permanent des données relatives à leur clientèle. Et de ce fait, ces gisements de données (et, en particulier, les mégabases de données comportementales, destinées à permettre le "data mining" [19]) vont faire de plus en plus l'objet d'une commercialisation à grande échelle dans laquelle la donnée personnelle deviendra véritablement une marchandise ayant une valeur marchande [20].

Face à cette réalité qui s'affirme chaque jour un peu plus, la tendance va être de demander aux entreprises d'assumer une part croissante de responsabilité. Selon une enquête menée aux Etats-Unis en 1998 si 81% des utilisateurs de l'Internet et 79% de ceux qui s'adonnent au commerce électronique considèrent que la protection de leur vie privée à l'occasion de ces communications électroniques est une préoccupation importante, une majorité encore plus importante de ces utilisateurs (91% et 96%) sont demandeurs d'engagements précis des entreprises commerciales présentes sur le Web en ce qui concerne l'usage des données collectées [21].

Cette reconnaissance du rôle croissant des entreprises et des demandes de protection accrue qui leur sont adressées, se traduit - notamment - par le fait que des systèmes juridiques traditionnellement peu favorables à légiférer sur les activités privées s'interrogent aujourd'hui sur la nécessité de prévoir des dispositions législatives applicables aux entreprises. C'est notamment le cas du Canada, qui disposant déjà d'une loi applicable aux informations détenues par les autorités fédérales, envisage d'adopter "une loi sur la vie privée applicable au secteur privé" [22]. Mais si chacun s'accorde à considérer que les entreprises doivent être mises à contribution, reste à trouver les mécanismes appropriés pour qu'elles assument leurs responsabilités en la matière.

3.2. La volonté de rechercher des mécanismes apparemment peu contraignants à l'encontre des entreprises

Bien que chacun identifie aujourd'hui les entreprises comme les principaux acteurs de la collecte et de la circulation mondiale des données personnelles, il semble que tant en Europe au travers de la directive 95/46 que sur le continent américain, la tendance soit plutôt à une approche libérale en ce qui concerne les mécanismes devant s'appliquer aux entreprises privées.

Dans la directive d'octobre 1995, nous avons déjà indiqué que la procédure de notification (qui est, en quelque sorte, la continuation de ce que la loi française de 1978 connaissait sous la dénomination de "déclaration") est destinée à devenir la référence de principe. Mais ce texte va plus loin en prévoyant une possibilité de

---

[19] Cf. notamment sur ce sujet, Claude Bourgeos, "Les mégabases de données comportementales et la protection des données personnelles", Droit de l'Informatique et des Télécoms, n° 98/2, pp. 6-13.

[20] Présentant en 1997 une proposition de loi sur la protection des données, le sénateur Dianne Feinstein constatait : "Our private lives are becoming commodities with tremendous value in the marketplace" (cité in Time Magazine, 2 juin 1997, p. 63).

[21] Résultats de l'enquête "E-Commerce & Privacy : A Survey of the American Public" menée par Louis Harris & Associates, Inc, rendus publics le 23 juin 1998 lors du US Department of Commerce Privacy Summit.

[22] Cf. notamment, Commissaire à la protection de la vie privée du Canada - Rapport annuel 1997-1998, Ministère des Travaux publics et Services gouvernementaux, Canada, 1998.

dispense de notification lorsque l'entreprise aura mis en place un "détaché à la protection des données à caractère personnel" (article 18.2). De même, cette directive consacre son chapitre V aux "codes de conduite" que les Etats membres et la Commission doivent encourager, notamment dans le contexte d'organisations professionnelles sectorielles [23].

Ces orientations, visant à alléger au maximum le poids des contraintes administratives s'appliquant sur les entreprises pour favoriser l'auto-régulation et l'auto-discipline des acteurs privés, sont évidemment en phase avec l'approche beaucoup plus libérale de ces questions qui prévaut outre-Atlantique. On sait que traditionnellement, les Etats-Unis sont hostiles par tradition politique et juridique à toute restriction du "free flow of information" et s'efforcent toujours de promouvoir officiellement une alternative reposant sur les initiatives du marché. Mais, cette réticence envers des systèmes administratifs contraignants a également cours, avec des nuances, dans l'ensemble de l'Amérique du Nord et le Commissaire canadien à la protection de la vie privée pouvait écrire, qu'à l'inverse de différentes législations européennes qui prévoient l'inscription (c'est-à-dire, la déclaration préalable) des traitements des entreprises auprès d'une autorité centrale, il lui semble que "l'inscription serait un exercice inutilement coûteux et bureaucratique qui monopoliserait à mauvais escient des ressources, lesquelles pourraient être mieux utilisées à défendre les intérêts relatifs à la vie privée" [24].

Pour simplifier, cette approche non contraignante débouche sur trois types d'instruments. La première catégorie - déjà évoquée - est celle des codes de conduite qui peuvent être établis par des organisations sectorielles [25], des groupes de réflexion ou d'intérêts [26] ou encore directement par chaque entreprise. Le deuxième niveau (qui peut fort bien se combiner avec le premier) concerne l'établissement d'un arrangement contractuel direct (y compris, en ligne) entre client et fournisseur pour régir les conditions d'exploitation des données personnelles liées à la transaction commerciale concernée. Enfin, certains grands opérateurs américains sur l'Internet se sont engagés - avec certains de leurs homologues européens et asiatiques - dans la voie de la spécification de standards techniques qui pourraient être intégrés dans les outils logiciels du marché et qui permettraient aux utilisateurs des réseaux de "comparer automatiquement les exigences des utilisateurs aux garanties offertes par les sites en matière de protection des données" [27]. Mais cette dernière approche (pour aussi séduisante qu'elle soit) qui est parfois présenté dans la communauté de l'Internet pour la solution ultime et définitive à la question de la protection des données, n'est généralement considérée en

[23] Il s'agit là d'une approche qui est assez nouvelle en France s'agissant de la question des données nominatives (on ne connaît que le code de déontologie du marketing direct de 1993 en la matière) mais qui a déjà été prônée en ce qui concerne la régulation de l'Internet.

[24] Commissaire à la protection de la vie privée du Canada - Rapport annuel 1997-1998, op. cit..

[25] Pour une analyse de ce mécanisme d'autorégulation sectoriel, cf. le document de travail "Evaluation des codes d'autoréglementation sectorielle : quand peut-on dire qu'ils contribuent utilement à la protection des données dans un pays tiers ?", Commission européenne, Groupe de protection des personnes à l'égard du traitement des données à caractère personnel, DG XV D/5057/97, WP 7 du 14 janvier 1998.

[26] Citons, par exemple, s'agissant de la protection des données personnelles sur l'Internet, les "Electronic Privacy Principles" élaborés en 1996 par le Cyber-Rights Working Group du "Computer Professionnals for Social Responsibility" (CSPR).

[27] Cf. CNIL, 18ème rapport, p. 130.

Europe que comme une contribution potentiellement utile à l'information des consommateurs mais insuffisante en soi pour assurer à elle seule cette protection et comme pouvant induire en erreur les entreprises opératrices sur le niveau réel de leur responsabilité [28].

3.3. La nécessité d'intégrer ces nouvelles responsabilités dans un cadre nouveau du droit de l'entreprise

Mais quel que soit l'instrument utilisé, dès lors que la loi et/ou le marché vont reconnaître un rôle croissant aux entreprises dans la gestion et la protection des données personnelles, cela va nécessairement se traduire par une plus grande responsabilité juridique de ces entreprises en la matière. Comme le soulignait, par exemple, dès 1996 le Professeur Herbert Maisl, l'application de la directive de 1995 plus orientée vers l'intervention a posteriori des organismes de contrôles, devrait, par exemple, se traduire en France par des investigations de la CNIL qui "permettraient de régler les questions à l'amiable mais également de faire davantage jouer le dispositif pénal prévu en 1978 et aujourd'hui intégré dans le code pénal" [29]. Mieux encore, la directive prévoit au profit de la personne fichée (et donc, indirectement, à l'encontre des entreprises qui la fichent) une obligation supplémentaire d'information (qui n'existait pas dans la loi française de 1978) lorsque la collecte n'a pas été réalisée directement auprès d'elle (par exemple en cas de cession de fichiers) [30].

L'accroissement de la responsabilité des entreprises - qu'elle soit pénale, délictuelle ou contractuelle - en matière de gestion des données personnelles sera donc vraisemblablement la contrepartie logique d'une législation qui fera plus appel à l'autoréglementation et aux contrôles a posteriori qu'à la mise en oeuvre de procédures administratives contraignantes. Dès lors, il va être encore plus important pour les entreprises qu'elles intègrent, mieux que par le passé, cette exigence de protection dans leur dispositif juridique interne.

Si l'on veut se livrer à quelques anticipations, on peut penser que cette problématique des données personnelles - dont nous avons vu plus haut qu'elle demeurait jusqu'à présent très à l'écart des catégories juridiques du droit de l'entreprise - pourrait mieux s'intégrer à de nouvelles dimensions émergentes des pratiques (et donc, du droit) d'entreprise.

---

[28] Cf. l'avis du groupe de travail de la Commission européenne sur le projet P3P (Platform for Privacy Preferences) qui relève, notamment, "que le risque existe que le P3P, une fois intégré à la nouvelle génération de logiciels de navigation, puisse induire en erreur les opérateurs implantés dans l'UE en leur faisant croire qu'ils peuvent être déchargés de certaines de leurs obligations légales" (Commission européenne, Groupe de protection des personnes à l'égard du traitement des données à caractère personnel, Avis 1/98, XV D/5032/98, WP 11 du 16 juin 1998). On voit ici reparaître la tentation des entreprises - déjà évoquée plus haut - de voir dans tout procédé préventif un certificat de conformité les exonérant de leur responsabilité ultérieure.

[29] Herbert Maisl, "Changer la CNIL ? Pour quoi faire ?", in Monique Linglet (dir.), Expertises pour l'an 2000 - Vers un droit du numérique, Editions des Parques, 1996, p. 76.

[30] A l'inverse, la jurisprudence française affirmait - contrairement à la position alors défendue par la CNIL - que la loi de 1978 ne faisait aucunement obligation d'avertir la personne fichée lorsque la collecte avait été effectuée auprès d'un tiers (Cass. Crim., 25 octobre 1995, Centrale professionnelle sur les impayés, Droit de l'Informatique et des Télécoms, n° 98/2, p. 43).

La première de ces dimensions nouvelles est assurément celle de la sécurité de l'entreprise. On a décrit ailleurs en quoi il apparaît nécessaire (et sans doute inévitable, dans une économie mondialisée et fortement concurrentielle) que se développe un véritable droit de la sécurité économique des entreprises [31]. Or, indiscutablement, la nécessité de protéger les données personnelles traitées par l'entreprise (qui est déjà - en droit français - traduite en obligation juridique de sécurité [32]) va globalement dans le même sens que l'impératif plus large de sécurité et de responsabilité qui va s'imposer de plus en plus aux entreprises (ou va leur être imposé, tant par leurs partenaires économiques que par leurs clients ou leurs salariés) [33].

Plus largement encore, on peut envisager que le mouvement actuel en faveur d'une plus grande "moralisation" des pratiques économiques (notamment, par la criminalisation croissante de différentes formes d'agissements anticoncurrentiels, comme la corruption [34]) donne une consistance juridique réelle à la notion, encore actuellement imprécise, d'"éthique d'entreprise" [35]. Si tel était le cas, il est clair également que les préoccupations relatives à l'usage des données personnelles constitueraient (pour les entreprises européennes tout au moins) un volet important de cette nouvelle branche du droit de l'entreprise.

Établi il y a vingt ans pour des motifs sans rapport avec les impératifs économiques ou commerciaux et plutôt destiné, à l'origine, à encadrer les pratiques de l'État, le droit des données nominatives en France n'a pas été sans effet sur les entreprises privées. Bien au contraire, on peut considérer qu'aujourd'hui, la plupart des questions majeures en la matière concernent la pratique des entreprises (notamment du fait de la mondialisation croissante des échanges économiques et du développement des réseaux électroniques de type Internet) et imposent de leur donner une place croissante dans le dispositif de protection.

Mais dans le même temps, il paraîtrait difficile de soumettre les acteurs économiques privés à plus de contraintes administratives qu'ils n'en ont connues dans le passé. C'est pourquoi la directive de 1995 ne revient sur le caractère purement déclaratif

---

[31] Cf. Bertrand Warusfel, "Intelligence économique et sécurité de l'entreprise", Cahiers de la sécurité intérieure, n° 24, 2ème trimestre 1996 (republié par Problèmes économiques, décembre 1996).

[32] Par les articles 7 de la convention du Conseil de l'Europe et 29 de la loi du 6 janvier 1978.

[33] On soulignera cependant, à nouveau (cf. supra), que dans certains cas la sécurisation des échanges commerciaux de l'entreprise peut aller à l'encontre de la protection de l'anonymat et de la vie privée des personnes. Mais, même dans ce cas, la contradiction n'est qu'apparente, car dès lors que plus de sécurité pour l'entreprise impose plus de collecte de données personnelles, cela implique du même coup plus d'obligations pour l'entreprise d'assurer la sécurité et la confidentialité de ces données. Les deux niveaux de sécurité vont donc finalement dans le même sens, du point de vue de l'entreprise.

[34] Cf. en particulier l'adoption en décembre1997 de la convention OCDE contre la corruption des agents publics étrangers à l'occasion des transactions commerciales internationales.

[35] Il existe, en cette matière, une vive controverse doctrinale (et philosophique) entre ceux qui considèrent que le domaine de l'éthique doit, par nature, demeurer en-deçà ou à côté de la sphère juridique et ceux qui estiment que, même si les élaborations éthiques ou déontologiques relèvent d'une certaine forme de "*soft law*", elles s'intègrent nécessairement dans une dimension juridique, ne serait-ce qu'au titre de source supplétive du droit positif.

des procédures qu'en ce qui concerne les traitements les plus sensibles (pour lesquels l'examen préalable donnera aux entreprises la sécurité juridique qui leur manquait) et cherche plutôt, pour le reste, à s'aligner sur la position libérale dominante.

Il n'en demeure pas moins que dans ce nouveau contexte d'une économie mondiale de l'information et de la circulation quasi-généralisée des données personnelles via les réseaux électroniques, l'autorégulation des acteurs et les chartes déontologiques qu'ils proposeront ne pourraient pas cacher la responsabilité croissante que toutes les entreprises vont devoir assumer dès lors qu'elles collecteront, traiteront ou commercialiseront des données personnelles. Dans ce domaine, comme dans d'autres, la responsabilité juridique et les inévitables contentieux qui en découlent sont la contrepartie d'une plus grande liberté économique et commerciale pour les entreprises. Reste, dans ce nouveau contexte où les pratiques d'entreprise et l'intervention des juges seront dominantes, à s'interroger sur la place que conserveront les autorités administratives de contrôle nationales (comme la CNIL française) et plus largement sur le rôle que les pouvoirs politiques - en charge de la protection des libertés individuelles et collectives - pourront y jouer.

Bertrand WARUSFEL