

**« PRINCIPES DES LEGISLATIONS  
DE PROTECTION DES DONNEES PERSONNELLES »**

*Par Mme Sophie VULLIET-TAVERNIER*

-----

Comme l'a souligné Mme Isabelle FALQUE-PIERROTIN, une législation de protection des données repose aujourd'hui sur quatre piliers qui sont fondamentaux :

- L'élaboration de principes de protection des données, principes que l'on retrouve aujourd'hui dans la plupart des instruments juridiques internationaux et notamment européens en matière de protection des données. Ces principes ont pour objet d'encadrer l'utilisation de l'informatique et de fixer un certain nombre de garanties et de droits au profit des personnes, mais également des obligations vis-à-vis des responsables de traitement ;

- L'institution d'un certain nombre de droits pour les personnes fichées ;

- Troisième élément clef, l'institution d'un mécanisme de sanction en cas de non respect des principes ou des droits des personnes ; et

- Quatrième élément clef, l'institution d'une autorité de contrôle indépendante, chargée de veiller au respect des principes, au respect des droits à la protection des données. Cette autorité de contrôle doit être dotée de pouvoirs de contrôle et de sanction.

Avant d'aborder ces principes de protection des données, je voudrais tout d'abord faire un point sur les notions clés de protection des données, et tout d'abord sur la notion de données personnelles. Qu'entend-on par « données à caractère personnel » ?

1. Il s'agit de toute information se rapportant à une personne physique. La loi de protection des données ne s'applique pas aux fichiers d'entreprises, elle ne concerne que l'individu. Il s'agit fondamentalement de protéger les personnes physiques à l'égard du traitement informatique de leurs données.

2. Cette information permet d'identifier directement ou indirectement une personne. Quand on parle d'identification directe, il s'agit par exemple d'enregistrer

dans une base de données le nom et le prénom d'une personne. Lorsqu'il s'agit d'identifier de façon indirecte une personne physique, c'est par exemple enregistrer son numéro de téléphone, un numéro d'immatriculation comme le numéro d'immatriculation sociale par exemple. . Cela peut être également, par exemple, le numéro d'immatriculation de sa voiture, puisque ce numéro est enregistré dans un fichier comportant le nom du propriétaire du véhicule. Le fichier en question relève donc de la loi de protection des données. De la même façon, quand on parle d'identification indirecte des personnes, ce peut être une identification par des éléments physiques, spécifiques qui leur sont propres. Par exemple, l'empreinte digitale d'une personne est une donnée qui peut permettre de l'identifier. C'est ce qu'on appelle une donnée biométrique. Dans le monde Internet également, l'adresse IP permet d'identifier l'ordinateur lorsqu'il se connecte sur Internet. Cette adresse IP peut également permettre d'identifier l'individu qui est derrière la machine.

Cette notion de données à caractère personnel est une notion extrêmement large, d'où un champ d'application des lois de protection des données très étendu.

Deuxième notion clés : la notion de « fichiers » et de « traitement ». Par « fichier », on entend tout ensemble structuré d'informations accessibles selon des critères déterminés. Concrètement, un registre du personnel qui doit comporter le nom du salarié, sa situation professionnelle, des éléments de sa paye, constitue un fichier qui est structuré. De la même façon, un annuaire téléphonique qui comporte les noms, des numéros de téléphone... constitue un fichier. Au-delà, la loi de protection des données s'intéresse de façon plus générale à la notion de traitement de données à caractère personnel. Par « traitement de données », on entend tout ensemble d'opérations se rapportant à la collecte, à la saisie informatique des données, au stockage des informations, à la consultation, à l'interconnexion ou au rapprochement d'informations. Là aussi le champ d'application et d'intervention des législations de protection des données est extrêmement large. Il couvre non seulement les bases de données classiques, , mais également par exemple toutes les applications de cartes à puce et toutes les applications fonctionnant sur Internet : (sites web, applications de commerce électronique, réseaux sociaux (comme facebook, etc..., le dossier médical sur Internet...).

Troisième notion clé, c'est la notion de « responsable de traitement ». Par « responsable de traitement », on entend l'organisme, le maître du fichier qui va décider de l'informatisation des données personnelles, des moyens informatiques à

utiliser (par exemple réseau Internet, mise en place d'une base de données centralisée) et sera ensuite responsable en cas de non respect des principes fondamentaux de protection des données. Cette notion de responsabilité est aussi un principe clé dans l'ensemble des législations de protection des données. Concrètement, si le Ministère de la Justice, par exemple, décide d'informatiser l'état civil, il sera responsable de la constitution de ce fichier central. Il sera responsable en cas de dysfonctionnement du fichier, de divulgation d'informations ou d'utilisation détournée de ces informations.

Le responsable du traitement est aussi celui qui est établi sur le territoire de l'État considéré, ou qui recourt à des moyens de traitement, c'est-à-dire l'utilisation de moyens informatiques situés sur le territoire de l'État considéré.

Venons-en maintenant aux principes fondamentaux. Ces principes fondamentaux sont au nombre de cinq, donc cinq règles d'or qui sont aujourd'hui communes à l'ensemble des législations de protection des données.

C'est tout d'abord le respect du principe de finalité qui veut que lorsqu'on met en place une application informatique qui va enregistrer des informations sur les personnes, celle-ci correspond à un objectif déterminé et légitime correspondant aux missions de l'organisme. Ceci veut dire que par exemple un fichier de gestion du personnel ne peut en aucun cas être utilisé à des fins commerciales. De la même façon, un fichier d'État civil ne peut être utilisé à des fins de prospection politique ; un fichier médical comportant des données médicales sensibles ne peut en aucun cas être utilisé par des compagnies d'assurances...

Le respect du principe de finalité suppose qu'un mécanisme de sanction soit prévu lorsque l'on constate un détournement de l'usage du fichier. En France, le Code pénal prévoit des sanctions pénales lourdes en cas de détournement de finalité, puisqu'elles peuvent aller jusqu'à cinq ans d'emprisonnement et 300 000 € d'amende.

Deuxième principe clé, c'est le principe de pertinence des données qui veut que lorsqu'on enregistre des données dans un fichier, ces informations soient adéquates par rapport à l'objectif recherché.

De façon générale, les lois de protection des données prévoient également un encadrement particulier pour certaines catégories d'informations jugées plus sensibles que d'autres. C'est notamment le cas des données relatives aux origines raciales ou ethniques des personnes, à leur appartenance religieuse, syndicale et également à leur

appartenance politique. L'enregistrement de ces données est en effet interdit, sauf dérogations prévues expressément par la loi. Il en est de même également en ce qui concerne les données relatives à la santé et à la vie sexuelle. Là aussi, le législateur encadre très strictement l'utilisation des données et, de façon générale, réserve l'enregistrement et le traitement de ces derniers notamment aux professionnels de santé agissant dans le cadre de l'exercice de leur profession.

Pourquoi un encadrement aussi strict pour ce type de données ? Pour éviter le risque de discrimination liée à un usage abusif des fichiers de traitement. Certaines législations prévoient aussi un encadrement particulier en ce qui concerne l'utilisation de l'identifiant national, comme le numéro de sécurité sociale en France par exemple, dans le souci d'éviter les interconnexions généralisées de fichiers de traitement. . En France, le numéro de sécurité sociale ne peut en aucun cas être utilisé dans les fiches de police ou dans les fichiers bancaires. Donc à chaque sphère d'activité son identifiant sectoriel. Ainsi, les fichiers fiscaux comportent un identifiant spécifique . Toute utilisation illicite de ces informations sensibles est également passible de sanctions pénales lourdes.

Le troisième principe fondamental est celui du droit de l'oubli. Ce droit se traduit, dans les lois de protection des données, par la nécessité d'instaurer une durée de conservation limitée des informations dans les traitements et dans les fichiers, et par une obligation de mise à jour des informations. La durée de conservation doit être graduée et limitée en fonction de la finalité du fichier. Par exemple, la CNIL préconise que la durée de conservation des données dans les fichiers de clients, qui sont utilisés à des fins de prospection commerciale, ne dépasse pas un délai d'un an après la dernière opération de prospection commerciale. De la même façon, s'agissant des fichiers de police, la Commission a obtenu du Ministère de l'intérieur que ces durées de conservation soient graduées, limitées en fonction du degré de gravité de l'infraction et également de l'âge de la personne. Au-delà de cette durée de conservation, les informations doivent être selon le cas archivées ou effacées.

Autre cas également, s'agissant d'Internet : la législation française restreint la durée de conservation des données dites de trafic pour les opérateurs de télécommunications et également les fournisseurs d'accès Internet. Elle réduit la durée de conservation des données de trafic à un an maximum. Le fait de conserver au-delà de la durée de conservation prévue les informations constitue également une infraction pénale passible de sanctions lourdes.

Quatrième principe : l'obligation de sécurité, est à la charge des responsables de traitement. Elle les oblige à prendre toute précaution, toute mesure pour garantir la confidentialité des données personnelles, éviter leur divulgation et également garantir l'intégrité des informations qui sont enregistrées. En pratique, ceci nécessite la mise en place de mesures de sécurité à la fois physique, organisationnelle et également des mesures de sécurité logique. Par exemple, des procédures de contrôle d'accès par mots de passe individuels aux fichiers, mise en place de procédures d'habilitation... qui sont particulièrement importantes par exemple lors qu'il s'agit de mettre en place des fichiers médicaux où il faut vérifier qu'il n'y ait pas de failles de sécurité, que seules des personnes bien habilitées aient accès à ces informations sensibles.

En France, la CNIL a eu à se prononcer, à titre expérimental, sur ce qu'on appelle le dossier médical personnel sur Internet, qui est hébergé par des prestataires privés et qui est consultable directement sur Internet. Il est évident que cette consultation sur Internet, compte tenu des risques de divulgation inhérents à l'utilisation de ce réseau, comporte des risques majeurs, d'où la nécessité de protéger de façon très rigoureuse les accès à ce dossier médical personnel et de le sécuriser de façon appropriée. Ceci passe notamment par la mise en place de procédures d'identification et d'authentification individuelles des professionnels de santé, par exemple, titulaires de cartes à puces. Ceci passe également par des mesures de cryptage, de chiffrement des informations, des bases de données qui vont être hébergées par des prestataires privés. Au-delà, la législation française interdit toute utilisation commerciale des données de santé et tout défaut de sécurité est passible de sanctions pénales lourdes.

Le cinquième et dernier principe est le respect des droits des personnes qui se traduit par une obligation de transparence. Tout responsable de traitement, tout ministère et toute entreprise qui informatise son fichier, qui met en place sur Internet une application de commerce électronique ou qui informatise son fichier de personnel, doit informer les personnes concernées de cette informatisation, des conditions d'utilisation de leurs données, des destinataires des informations.

Lorsqu'il s'agit de collecter ces informations sur des questionnaires, les questionnaires doivent comporter un certain nombre de mentions pour informer les personnes de leurs droits et des destinataires des informations : ces personnes doivent avoir connaissance des informations les concernant, figurant dans les bases de données sur Internet. Ainsi, le droit d'accès aux informations est le droit de connaître le

contenu des informations enregistrées sur son compte, le droit de les faire rectifier si elles s'avèrent inexactes, périmées ou incomplètes. C'est également le droit de s'opposer, sous certaines conditions, à l'informatisation de ces données.

Ce droit de s'opposer comporte quelques restrictions, lorsqu'il s'agit par exemple de prévoir un enregistrement de données dans des fichiers pour lequel il y a une obligation légale d'y figurer. (par exemple les fichiers de l'administration fiscale). Dans ces cas, la loi prévoit bien évidemment une dérogation à cette obligation. Au-delà de cela, l'ensemble des législations de protection prévoient en contrepartie un droit de s'opposer sans avoir à justifier de raisons légitimes à l'utilisation de ces données à des fins commerciales. . C'est le rôle fondamental des autorités de protection des données de veiller à l'application pratique de ces droits.

Je voudrais en terminer par le droit d'accès indirect aux données enregistrées dans les fichiers de police. Les lois de protection des données peuvent prévoir des dérogations à l'exercice du droit accès direct. C'est notamment le cas lorsqu'il s'agit par exemple de savoir si on est fiché dans un fichier de police. En France, la Commission nationale Informatique et Liberté joue un rôle de médiation à cet égard, c'est-à-dire qu'une personne qui souhaite savoir si des données la concernant sont enregistrées dans un fichier de police, peut s'adresser auprès de la Commission, qui va alors entreprendre pour le compte du requérant les vérifications auprès du Ministère de l'Intérieur, par exemple. Ce n'est qu'avec l'accord du ministère concerné que la Commission communiquera ensuite à l'intéressé les informations lui concernant.