

« LES AUTORITES DE PROTECTION DES DONNEES ET LEURS RELAIS »

Par Mme Sophie VULLIET-TAVERNIER

Présentation des autorités de protection des données : leur statut, leur composition, leur pouvoir de contrôle, de conseil et également de sanctions.

Pourquoi est-il nécessaire dans une législation de protection des données de disposer d'une autorité indépendante de contrôle et de protection des données à caractère personnel ? Il y a en effet deux raisons essentielles :

- D'une part, il s'agit d'assurer la transparence et le contrôle de l'informatisation de différents secteurs privés, mais également le contrôle de l'informatisation des grands fichiers administratifs et de l'ensemble des bases de données administrative ;
- D'autre part, c'est la nécessité de disposer d'un organe capable de s'adapter face aux évolutions technologiques, d'effectuer une veille technologique et également capable d'intervenir en cas de plainte et en cas de non-respect des dispositions de la loi de protection des données.

Qu'entend-on par l'autorité de contrôle indépendante ? On peut dire qu'il y a quatre critères principaux pour déterminer si une autorité de contrôle est véritablement indépendante :

1°) Le premier de ces critères est le mode de désignation de ses membres ou du titulaire. En effet, lorsqu'on effectue un panorama des législations de protection des données, les autorités de protection des données sont soit des organes collégiaux, soit des commissaires à la protection des données. S'agissant des autorités francophones de protection des données, il y a en 9 autorités sur les 24 qui ont une composition pluraliste et collégiale.

Le mode de désignation doit garantir l'indépendance de la commission. Pour ce faire, les membres sont en général désignés soit par les Parlements ou par les

hautes juridictions ou encore par les plus hautes autorités de l'État. En Italie par exemple, c'est le Parlement qui désigne les membres de la Commission italienne de protection des données. Le mode de désignation en France est très pluraliste puisque les membres de la Commission sont d'une part de hauts magistrats (désignés respectivement par les plus hautes juridictions administrative, judiciaire et financière), et d'autre part quatre parlementaires, deux membres du Conseil économique et social et cinq personnalités qualifiées, désignées notamment en raison de leurs compétences en informatique et dans le domaine des libertés individuelles.

2°) Le deuxième critère d'indépendance est le fait que les membres de l'autorité de protection des données sont inamovibles. Pendant la durée de leur mandat, ils ne peuvent être démis de leur fonctions

3°) Le troisième critère d'indépendance est le fait qu'il existe des incompatibilités avec l'exercice de certaines fonctions. On ne peut pas à la fois être membre du Gouvernement ou diriger une société de services en informatique, par exemple, et être membre de l'autorité de protection des données. C'est un point tout à fait essentiel.

4°) Le quatrième critère est la nécessité de disposer de moyens financiers suffisants. Ce qui veut dire que, selon le cas, il s'agit d'un budget propre à l'autorité de protection des données, qui est alloué sur le budget de l'État. L'autorité peut également être financée par des redevances. Mais il est essentiel qu'elle dispose de moyens autonomes.

Enfin, et c'est un dernier aspect qu'il faut souligner, l'autorité de contrôle doit être transparente vis-à-vis du citoyen, du Gouvernement et des entreprises. Pour ce faire, elle doit remettre un rapport annuel d'activité aux plus hautes autorités de l'État. Sur l'aspect financier, ses comptes sont soumis au contrôle. Quant à l'autorité française, elle est soumise au contrôle *a posteriori* de la Cour des Comptes, la plus haute juridiction financière.

Si l'on prend l'exemple de la CNIL, elle est une autorité administrative indépendante composée de 17 membres : hauts magistrats, parlementaires, conseillers économiques et sociaux et personnalités qualifiées. En outre, le président ainsi que les deux vice-présidents de la CNIL ne sont pas nommés par le Gouvernement mais élus

par les autres membres de la commission. Dans la loi française de protection des données, il est également spécifié que les membres de la commission ne reçoivent d'instructions d'aucune autorité publique. Tout au contraire, les entreprises et les administrations doivent prendre toute mesure pour faciliter l'action de la commission, notamment son action de contrôle. Il faut rappeler aussi que, dans la législation française, toute entrave à l'action de la commission est constitutive d'un délit.

La CNIL ? En effet, cette commission dispose d'un budget de 13 millions d'euros. Outre les 17 membres, elle dispose de services : actuellement, plus de 120 personnes, à la fois des juristes, des informaticiens, qui sont là pour contribuer à l'expertise juridique et technologique des membres de la commission.

Quelles sont les missions de l'autorité de protection des données ? De façon générale, ces missions sont de 3 ordres :

- mission d'information, de conseil et d'expertise, à la fois à des professionnels du secteur, du grand public, des administrations ;
- mission de contrôle à la fois en amont, au travers notamment des déclarations de fichiers, et en aval par des missions de contrôle sur place pour vérifier leur conformité par rapport aux principes de protection des données ;
- pouvoir de sanction en cas de non-respect de la loi.

1°) Mission d'information, de conseil et d'expertise : Cette mission d'information s'exerce par le biais des actions de sensibilisation, de communication que les autorités peuvent effectuer auprès de publics divers, des entreprises et de certains secteurs professionnels ciblés et également des communes, des administrations et des jeunes. À cet égard, si l'on prend l'exemple de la commission française, nous avons engagé des actions de partenariat avec le ministère de l'Education nationale, de façon notamment à sensibiliser les jeunes dans les écoles sur les risques liés à Internet, à la diffusion sur les blogs, sur les réseaux sociaux (comme facebook, par exemple) d'informations trop personnelles qui peuvent porter atteinte à la vie privée des jeunes plus tard, notamment lorsqu'il s'agit de postuler à des emplois. Nous participons également à des colloques et des formations. Nous diffusons en outre un certain nombre de guides pratiques pour aider les citoyens à mieux connaître leur droit à la protection des données et pour sensibiliser les secteurs

professionnels à leurs obligations au regard de la loi de protection des données. Par exemple, nous diffusons un guide concernant le droit d'accès. C'est un guide pratique avec des modèles de lettres pour demander, par exemple, à exercer son droit d'accès. Nous avons aussi un guide destiné aux clients des banques et des organismes de crédit pour leur expliquer concrètement la façon dont ils sont fichés, la façon dont ils peuvent obtenir radiation de leurs coordonnées dans les fichiers établis par les établissements de crédits. Par ailleurs, nous avons un site Internet : www.CNIL.fr. Ce site donne un certain nombre d'explications concrètes sur les principes de protection des données et notamment sur les mesures de sécurité et d'information...

La deuxième mission importante dans le cadre de cette action de conseil : nous avons un corps d'experts techniques qui est régulièrement sollicité pour rendre des expertises techniques sur les projets informatiques dont nous sommes saisis. Par exemple, nous avons été saisis des grands projets informatiques, venant du Ministère de l'Intérieur pour la mise en place du passeport biométrique comportant les empreintes digitales.. la CNIL publie régulièrement des recommandations sur un certain nombre de sujets, par exemple sur les fichiers de recrutement, les dispositifs de vote électronique... Dans ces recommandations, un certain nombre de mesures de sécurité sont préconisées afin de garantir l'anonymat du vote. La Commission a également été amenée à émettre à collaborer à la mise en place de référentiels généraux de sécurité, dans le cadre du développement de l'administration électronique, recommandant des mesures de sécurité, telles que le cryptage des informations, des mesures d'identification et d'authentification des utilisateurs.

La CNIL joue aussi un rôle de conseil auprès du Gouvernement et du Parlement. Elle peut être saisie pour avis de tout projet de loi intéressant la protection des données personnelles (concernant les fichiers de crédit, la mise en place de grands fichiers de police...). La commission est aussi régulièrement auditionnée au Parlement dans le cadre de l'examen de projets de lois.

Enfin, pour terminer sur cette mission de conseil et d'expertise, depuis déjà quelques années, la commission a engagé des actions de concertation avec certains milieux professionnels, notamment avec les géants de l'informatique et de l'Internet comme Microsoft ou Google de façon à les sensibiliser sur les principes de protection des données. La Commission participe en amont à certains projets de recherche, notamment dans le domaine de la biométrie.

Une deuxième mission importante des autorités de protection des données est la mission de contrôle : un contrôle *a priori* et un contrôle *a posteriori*.

Traditionnellement, la mission de contrôle *a priori* s'exerce par le biais des obligations déclaratives. Dans l'ensemble des législations de protection des données, lorsqu'on met en place un traitement informatique portant sur des données personnelles, il y a nécessité de le notifier auprès de l'autorité de contrôle. Cette obligation déclarative s'impose, en principe, dès lors qu'il s'agit d'informatiser toute donnée comportant des éléments plus ou moins identifiants sur les personnes. En pratique, il est illusoire de vouloir effectuer un contrôle exhaustif sur l'ensemble des fichiers informatiques existants. Ce constat a été fait au niveau de l'ensemble des législations de protection des données et également au niveau européen (avec la directive européenne de 1995 dont on a parlé hier). Ce constat a conduit à une évolution des législations de protection des données, de façon à prévoir un allègement de ce mode de contrôle *a priori* ; c'est-à-dire que, concrètement, le choix a été fait d'alléger les formalités déclaratives et de réserver ce contrôle aux applications les plus sensibles.

Pour vous donner quelques chiffres concernant la CNIL, nous avons enregistré dans notre propre fichier plus de 1 200 000 déclarations de fichier, soit à peu près 72 000 déclarations par an. Cela peut paraître énorme mais pour autant il ne reflète pas l'état de l'informatisation de la société française. C'est une des raisons pour laquelle, le législateur français a estimé nécessaire de prévoir au profit de la CNIL un pouvoir d'exonération pour certaines catégories de fichiers ou de traitements qui sont peu sensibles et qui ne portent pas atteinte à la vie privée ou aux libertés. C'est notamment le cas des fichiers de paie du personnel qui sont aujourd'hui exonérés de déclarations. C'est également le cas de tous les traitements informatiques d'annuaires du personnel ou qui n'ont pas à être déclarés. La loi prévoit également certaines exonérations, notamment pour ce qui concerne les fichiers des membres des partis politiques, des syndicats, des églises qui sont exonérés de par la loi de toute déclaration.

Au-delà de cela, les autorités de protection des données ont mis en place des mesures de simplification des formalités déclaratives pour certaines catégories de traitements courants, par exemple en matière de gestion du personnel. La CNIL mais également d'autres autorités de protection des données disposent d'un pouvoir réglementaire pour fixer des normes qui s'imposent aux organismes et entreprises

souhaitant mettre en place des fichiers conformes à cette réglementation. La CNIL a beaucoup développé cette approche normative et entend le développer très fortement dans l'avenir, sous une forme nouvelle : la labellisation. Il s'agirait de labelliser des produits, des logiciels qui seraient conformes aux principes de protection des données, dans le domaine de la sécurité informatique, (par exemple (logiciels de cryptage, d'anonymisation)).

Une autre orientation forte est une participation de plus en plus active aux travaux de normalisation au niveau international, aux travaux de l'ISO, qui s'est engagée dans un travail d'élaboration de normes en matière de protection des données. La CNIL et certaines autorités de protection des données participent activement à ces travaux.

Pour revenir à l'aspect « contrôle préalable » par les autorités de protection des données, conformément à ce que prévoit en Europe la Directive de 1995, il est prévu le maintien d'un contrôle plus lourd pour certaines catégories de fichiers qui sont jugés plus sensibles que d'autres. En France, c'est notamment le cas pour les applications biométriques, comme l'enregistrement des empreintes digitales, la reconnaissance des contours de la main, de la reconnaissance faciale également. Ces dispositifs sont soumis à autorisation directe de la CNIL. Il en est de même pour ce qui concerne les interconnexions de fichiers différents, qui sont également soumises à autorisation de la CNIL, et les applications qui recourent à l'utilisation de l'identifiant national sous certaines conditions. Ces traitements doivent être autorisés par la CNIL ou par un texte adopté après avis de la CNIL.

En France, la CNIL dispose en effet d'une compétence générale sur l'ensemble des fichiers, non seulement du secteur privé mais aussi du secteur public y compris l'ensemble des fichiers mis en œuvre dans le cadre des fonctions régaliennes de l'État. Ainsi, les fichiers fiscaux sont soumis au contrôle de la CNIL, les fichiers de police et de sécurité publique et l'ensemble des fichiers qui ont pour objet, la prévention, la recherche des infractions pénales. Ces fichiers doivent également être autorisés par un texte réglementaire selon le cas ou même par la loi, et sont soumis à avis préalable de la CNIL.

Voilà en ce qui concerne le contrôle préalable. Je voudrais dire un mot d'une institution tout à fait originale et récente dans la loi française de protection des données qui est le correspondant à la protection des données. Il s'agit d'une personne qui doit

être désignée au sein de l'entreprise ou de l'administration. Cette désignation, encore facultative aujourd'hui en France, permet à l'organisme qui s'en dote de diffuser localement la culture informatique et libertés, de permettre ainsi une meilleure application de la loi sur la protection des données. Cette institution existe également dans certains pays, notamment en Allemagne, en Suède.. A ce jour, plus de 5000 organismes privés comme publics en France ont désigné un correspondant à la protection des données. Le fait de désigner un correspondant permet également, sous certaines conditions, de dispenser de déclaration les entreprises. Dernier aspect : le contrôle *a posteriori*, c'est-à-dire la possibilité pour les autorités de protection des données de procéder à des vérifications sur place, des applications informatiques. Ce pouvoir de contrôle sur place a été très fortement renforcé en France par la loi de 2004 qui a modifié la loi informatique et libertés de 1978. Ce pouvoir permet à la CNIL d'accéder à tous locaux professionnels. Les agents de la CNIL qui procèdent à ces contrôles sont habilités et astreints au secret professionnel. Ils ont la possibilité de demander sur place tout document nécessaire, en prendre des copies, d'accéder aux programmes informatiques et aux données et de demander la communication de ces informations. La loi prévoit un certain nombre de restrictions, lorsqu'il s'agit d'accéder à des fichiers couverts par le secret professionnel, par exemple : des fichiers médicaux. Nous devons nous faire accompagner d'un médecin qui va accéder lui-même auxdits fichiers informatiques .

La loi prévoit également, sous certaines conditions, la possibilité pour le responsable du fichier de s'opposer à la mission de vérification. Nous avons l'obligation en informer le responsable du fichier, et en cas de refus du responsable du fichier de laisser la CNIL entrer dans ses locaux, nous pouvons faire appel au président du tribunal compétent qui va, par une ordonnance, autoriser la CNIL à procéder à cette mission de vérification sur place.

La CNIL a ainsi réalisé en 2008 plus de 200 contrôles aussi bien auprès des entreprises et des établissements de crédit, bancaires qu'auprès des communes, des administrations. Elle a en particulier conduit un important contrôle auprès du Fichier National de Police qui s'appelle en France le STIC, détenu par le Ministère de l'Intérieur.

D'une façon générale, les contrôles peuvent conduire à engager des procédures de sanction vis-à-vis des organismes concernés. Dans 25% des cas, ces contrôles ont débouché sur des procédures de sanction. Au préalable, je voudrais rappeler que ces

contrôles sont déclenchés soit sur plainte (la CNIL a reçu l'année dernière plus de 4000 plaintes), soit dans le cadre d'un programme annuel décidé par la Commission, soit encore sur auto-saisine.

Ces pouvoirs de sanction peuvent être à la fois des sanctions pécuniaires et administratives :

Le pouvoir de sanction pécuniaire : En France, la CNIL a la possibilité d'infliger des amendes qui peuvent aller jusqu'à 150 000 € et, en cas de réitération, jusqu'à 300 000 € dans la limite de 5% du chiffre d'affaires des entreprises. Ces sanctions pécuniaires ne sont pas applicables pour les traitements informatiques mis en place par l'État. La CNIL a également la possibilité d'enjoindre un organisme de cesser la mise en place d'un traitement informatique et de décider l'interruption du traitement et le verrouillage informatique des données. En cas d'atteintes graves et immédiates aux droits et libertés des personnes, le président de la CNIL peut demander, par la voie du référé, à la juridiction compétente d'ordonner toute mesure de sécurité nécessaire.

Dernier point, la CNIL peut saisir la justice, et dénoncer au Parquet les infractions à la loi de protection des données. Comme je l'ai évoqué hier, les sanctions pénales prévues par le Code pénal français en cas de non respect des dispositions de la loi de protection des données française sont extrêmes lourdes car elles peuvent aller jusqu'à 5 ans d'emprisonnement et 300 000 € d'amendes.

Pour finir, quelques statistiques s'agissant de l'activité de la CNIL : plus de 1 200 000 fichiers déclarés ; s'agissant des autorisations rendues: plus de 400 autorisations l'an dernier ; s'agissant des correspondants informatiques et libertés : plus de 5500 organismes ont désigné des correspondants ; plus de 4000 plaintes en 2008 dont la grande majorité concernent des problèmes de radiation des fichiers commerciaux (des usagers, des clients qui sont assaillis par des SPAM, des publicités dans leur boîte aux lettres et qui demandent la radiation des fichiers commerciaux) mais également des problèmes de mise à jour et de non-radiation dans les fichiers, des incidents de paiement de crédits aux particuliers et également dans le domaine du travail (la mise en place de dispositifs de cyber-surveillance sur les lieux de travail avec un contrôle abusif de l'activité des salariés. Les contrôles sur place ainsi que les plaintes ont débouché sur plus de quatre cents (400) mises en demeure préalables à la sanction, plus de 25 avertissements et 34 sanctions pécuniaires. (essentiellement dans

le secteur du crédit mais également vis à vis des opérateurs télécoms et de spammeurs, avec un montant de plus de 500 000 €à ce jour).