THEME L'IMMATERIEL ET LA PROTECTION DE LA PERSONNE

L'information est devenue une valeur importante dans l'activité économique. La constitution, l'enrichissement d'un fichier « prospects », « clients »… est un des exemples de cet enjeu. La collecte et le traitement des données (notamment à caractère personnel) sont favorisés par le développement des Nouvelles Technologies de l'Information et de la Communication (NTIC ou TIC). Cependant, le législateur veille au respect des droits et des libertés de la personne. La CNIL (Commission Nationale de l'Informatique et des Libertés), la Loi du 6 janvier 1978 permettent de contrôler et de sanctionner, le cas échéant, les abus en la matière.

1 - Définition des données à caractère personnel et des TIC

La loi du 6 Janvier 1978 (modifiée par la loi n° 2004-801 du 6 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), par le biais de son article 2 apporte une réponse explicite :
« Constitue une donnée à caractère personnel ***toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.*** *Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. […] ».*

Les **données sont donc considérées à caractère personnel** dès que les informations détenues permettent d'identifier directement ou indirectement une personne physique. Une personne est identifiée lorsque son nom apparaît dans un fichier (données nominatives). Une personne est identifiable lorsqu'un fichier comporte des informations permettant indirectement son identification.

Les données personnelles (ou nominatives) correspondent en général aux noms, prénoms, adresses (physique et/ou électronique), lieu et date de naissance, numéro de sécurité sociale….
Certaines de ces données sont qualifiées de « sensibles » (comme les données biométriques, le numéro de sécurité sociale…).
Ces données sont souvent considérées comme des données à risque, qu'il faut protéger impérativement.
Les NTIC génèrent elles aussi des données sur l'identité de l'internaute : on parle de **« données numériques personnelles ou traces numériques »** ; les cookies, par exemple, permettent d'obtenir des renseignements sur les habitudes de navigation des internautes. Ces cookies collectent des informations personnelles sans l'accord du visiteur d'un site.

2 - Traitement des « données à caractère personnel »

La loi du 6 Janvier 1978 (modifiée par la loi n° 2004-801 du 6 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), précise aussi dans son article 2 ce que l'on entend par **traitement des données à caractère personnel** :

« […]Constitue un traitement de données à caractère personnel ***toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.***
Constitue un fichier de données à caractère personnel tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés.
La personne concernée par un traitement de données à caractère personnel est celle à laquelle se rapportent les données qui font l'objet du traitement ».

3 - Règles de protection des droits de la personne

Les droits fondamentaux de la personne sont énoncés dans **l'article 2 de la Déclaration des droits de l'Homme et du Citoyen** du 26 août 1789 : *« Article 2 : Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'homme. Ces droits sont la liberté, la propriété, la sûreté et la résistance à l'oppression ».*

À cela, il faut ajouter l'article 12 de la Déclaration Universelle des droits de l'homme du 10 décembre 1948.

Art. 12 : *« 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 ».*

En outre, la notion de droits de la personne peut être comprise comme l'ensemble des droits subjectifs reconnus à la personne humaine, en tant que telle : les droits et libertés rattachés à la notion de liberté individuelle, et les droits spécifiques reconnus par la loi (droit au respect de la vie privée - article 9 du Code civil), droit au respect de la dignité de la personne (article 16) et du corps humain (articles 16-1 à 16-4)… ou par la jurisprudence (droit de s'opposer à la prise et à la reproduction de son image, rattaché par la Cour de cassation à l'article 9 du Code civil).

De manière plus précise, les personnes bénéficient donc de droits et de libertés qui sont protégés par le droit en toutes circonstances, y compris dans le cadre de l'utilisation d'outils informatiques. En France, **la Loi n° 78-17 du 6 janvier 1978**, connue sous le nom **« loi relative à l'informatique, aux fichiers et aux libertés »** est une loi qui a mis en place des règles de protection des droits de la personne lors de l'utilisation d'outils informatiques. Bien entendu, la loi a fait l'objet de modifications pour s'adapter à l'évolution des nouvelles technologies.

Dans son article 1, la loi relative à l'informatique, aux fichiers et aux libertés énonce que *« l'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».*

On peut, bien entendu, se référer à **l'article 9 du Code civil** : *« Chacun a droit au respect de sa vie privée ».*
Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée : ces mesures peuvent, s'il y a urgence, être ordonnées en référé ».

En outre, le Code pénal, à travers les articles 226-16 à 226-24, veille à l'application du respect des droits de la personne.

Au niveau communautaire, **le 28 janvier 1981, le Conseil de l'Europe** a adopté une **convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.** Cette Convention définit un certain nombre de principes de base :
- les données doivent être collectées et utilisées de manière loyale et licite,
- les données ne peuvent être collectées que dans un but précis et elles ne peuvent être utilisées que de manière compatible avec ce but,
- les données doivent être exactes, proportionnées et conservées uniquement pendant un délai nécessaire à la réalisation du projet,
- les données recueillies bénéficient d'un droit d'accès et de rectification par la personne concernée par la collecte.

Pour pouvoir ratifier la Convention, les États doivent garantir que leur législation nationale énonce ces principes de base à l'égard des données à caractère personnel relatives à tous les individus résidant sur leur territoire.

Une directive communautaire (N° 95/46) relative à la protection des personnes physiques et à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données a été adoptée le 24 octobre 1995.

La loi pour la confiance dans l'économie numérique (LCEN) du 21 juin 2004 qui a été élaborée dans la logique de la directive européenne du 8 juin 2000 sur le commerce électronique a institué un nouveau cadre juridique à l'environnement
Internet (institution d'une liberté de communication en ligne, encadrement du commerce électronique, publicité électronique et la lutte contre la cybercriminalité, différents acteurs (internautes, éditeurs…)).
À noter : la loi n° 2004-801(*) a modifié la loi de 1978 pour transposer en droit interne la directive de 1995. Cette loi de
2004 a renforcé les pouvoirs de sanction de la CNIL (Commission nationale de l'informatique et des libertés) et les droits des personnes physiques dont les données sont collectées.
(*) un premier décret d'application de cette loi est entré en vigueur (D n° 2005-1309 du 20/10/05), suivi d'un décret modificatif du 25 mars 2007 (D n° 2007-451) - **loi n° 2004-801 du 6 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.**

Une des règles fondamentales : il est interdit de créer un fichier (au sens de traitement de données à caractère personnel) sans le consentement de la personne concernée. De plus, il faut être informé du droit d'opposition et de rectification sur les données collectées.

4 - Obligations des responsables du traitement des données

La loi du 6 janvier 1978 modifiée prévoit certaines obligations à **la charge des responsables des fichiers et/ou traitements de données à caractère personnel** concernant : **la collecte, la finalité, la conservation, la sécurité, la confidentialité, l'information de la personne concernée et la déclaration.** Le non-respect de ces obligations est sanctionné au titre des articles 226-16 et suivants du Code pénal. **Les infractions** prévues à ces articles sont constitutives de **délits**.

- Obligation et déclaration des fichiers :
Certains traitements de données à caractère personnel doivent faire l'objet d'une **déclaration auprès de la Cnil** ou d'une autorisation de cette autorité administrative (voir site de la CNIL - *www.**cnil**.fr*). Les traitements informatiques de données personnelles qui présentent des risques particuliers d'atteinte aux droits et aux libertés doivent, avant leur mise en oeuvre, être soumis à l'autorisation de la CNIL.
Le non-accomplissement des formalités auprès de la CNIL est sanctionné de 5 ans d'emprisonnement et 300 000 € d'amende (*art. 226-16 du Code pénal*).

Art. 226-16
« Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.
Est puni des mêmes peines le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 2° du I de l'article 45 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ».

- Obligation et sécurité des fichiers
Tout responsable de traitement informatique de données personnelles **doit adopter des mesures de sécurité physiques** (sécurité des locaux), **logiques** (sécurité des systèmes d'information) et **adaptées** à la nature des données et aux risques présentés par le traitement. Il pourra s'agir notamment de restrictions d'accès aux locaux ou de mots de passe pour accéder aux fichiers, de pare-feu ou de tout autre programme de protection du système d'information.
Le non-respect de l'obligation de sécurité est sanctionné de 5 ans d'emprisonnement et de 300 000 € d'amende *(art. 226-17 du Code pénal).*

Art. 226-17
« Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en oeuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».

- Obligation et collecte des données
Le consentement de la personne dont les données sont collectées doit être recueilli pour utiliser une information l'identifiant.
Les données traitées doivent être exactes, complètes et tenues à jour. Hormis certains cas particuliers et limités, il est interdit de collecter des données sensibles.
On entend par **données sensibles**, les données concernant les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, ainsi que les données relatives à la vie sexuelle ou à la santé.
L'article 226-18 du Code pénal prévoit que la collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite est punie de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Art. 226-18
« Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».
Art. 226-18-1
« Le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».

- Obligation et durée de conservation
Les données à caractère personnel ne peuvent être conservées indéfiniment. En effet, la durée de conservation doit être fixée par le responsable. Le responsable d'un fichier fixe **une durée de conservation raisonnable** en fonction de l'objectif du fichier.
Le Code pénal sanctionne la conservation des données pour une durée supérieure à celle qui a été déclarée, de 5 ans d'emprisonnement et de 300 000 € d'amende (art. 226-20 du Code pénal).

Art. 226-19
« Le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'orientation sexuelle de celles-ci, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.
Est puni des mêmes peines le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée des données à caractère personnel concernant des infractions, des condamnations ou des mesures de sûreté ».

Art. 226-20
« Le fait de conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à la Commission nationale de l'informatique et des libertés, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la loi.
Est puni des mêmes peines le fait, hors les cas prévus par la loi, de traiter à des fins autres qu'historiques, statistiques ou scientifiques des données à caractère personnel conservées au-delà de la durée mentionnée au premier alinéa ».

- Obligation et finalité des traitements
Un fichier doit avoir **un objectif précis**.
Les informations exploitées dans un fichier doivent être **cohérentes par rapport à son objectif**.
Les informations **ne peuvent pas être réutilisées de manière incompatible avec la finalité** pour laquelle elles ont été collectées.
Tout détournement de finalité est passible de 5 ans d'emprisonnement et de 300 000 € d'amende *(art. 226.21 du Code pénal).*

Art. 226-21
« Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en oeuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».

- Obligation et confidentialité des données
Seuls sont autorisés à accéder aux données à caractère personnel contenues dans un fichier :
- **les destinataires explicitement désignés** pour en obtenir régulièrement communication,
- les « tiers autorisés » ayant qualité pour les recevoir de façon ponctuelle et motivée (ex. : la police, le fisc).
La communication d'informations à des personnes non-autorisées est punie de 5 ans d'emprisonnement et de 300 000 € d'amende.
La divulgation d'informations commise par imprudence ou négligence est punie de 3 ans d'emprisonnement et de 100 000 € d'amende *(art. 226-22 du Code pénal)*.

Art. 226-22
« Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.
La divulgation prévue à l'alinéa précédent est punie de trois ans d'emprisonnement et de 100 000 € d'amende lorsqu'elle a été commise par imprudence ou négligence.
Dans les cas prévus aux deux alinéas précédents, la poursuite ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droit ».

Art. 226-22-1
« Le fait, hors les cas prévus par la loi, de procéder ou de faire procéder à un transfert de données à caractère personnel faisant l'objet ou destinées à faire l'objet d'un traitement vers un État n'appartenant pas à la Communauté européenne en violation des mesures prises par la Commission des Communautés européennes ou par la Commission nationale de l'informatique et des libertés mentionnées à l'article 70 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».

- Obligation et information des personnes
Le responsable d'un fichier doit permettre aux personnes concernées par des informations qu'il détient d'exercer pleinement leurs droits. Pour cela, il doit leur communiquer : **l'identité du responsable du traitement, l'objectif de la collecte d'informations, le caractère obligatoire ou facultatif des réponses, les conséquences de l'absence de réponse, les destinataires des informations, les droits reconnus à la personne, les éventuels transferts de données** vers un pays hors de l'Union Européenne.
Le refus ou l'entrave au bon exercice des droits des personnes est puni de 1 500 € par infraction constatée et 3 000 € en cas de récidive *(art. 131-13 du Code pénal)*.

5 - Organes de contrôle et sanctions possibles

Dans un premier temps, la personne concernée par un traitement de données à caractère personnel, doit **s'adresser directement à la structure concernée** (entreprise, association, administration… sauf fichiers de police et gendarmerie).
Dans un deuxième temps, en cas de non-réponse, de réponse incomplète, la personne peut **saisir la CNIL** qui déclenchera une procédure d'intervention auprès de la structure concernée.

- Les contrôles de la CNIL
La CNIL a le pouvoir de contrôler l'ensemble des responsables de traitement de données. Ce pouvoir d'investigation est un moyen efficace pour vérifier l'application effective de la loi informatique et libertés.
Les missions de contrôle se déclenchent soit parce qu'elles :
- s'inscrivent dans le cadre d'un programme annuel de contrôles,
- répondent à des besoins précis (plaintes, demandes ...).

Pour contrôler les applications informatiques, la CNIL peut accéder à tous les locaux professionnels, demander communication de tout document nécessaire et d'en prendre copie, recueillir tout renseignement utile, accéder aux programmes informatiques et aux données.
La CNIL surveille par ailleurs la sécurité des systèmes d'information en s'assurant que toutes les précautions sont prises pour empêcher que les données ne soient déformées ou communiquées à des personnes non-autorisées.

- Les sanctions de la CNIL
La CNIL dispose de **différentes mesures et sanctions** pour faire respecter l'application de la loi :

En cas de manquements à la loi, la formation contentieuse de la CNIL peut prononcer :
1) **Un avertissement** à l'égard du responsable de traitement fautif, qui peut être rendu public.
2) **Une mise en demeure** à l'organisme contrôlé de faire cesser les manquements constatés dans un délai allant de dix jours à trois mois. Si le responsable de traitement se conforme à la mise en demeure, la procédure s'arrête et le dossier est clôturé.
Si le responsable de traitement ne se conforme pas à la mise en demeure de la CNIL, la formation contentieuse peut prononcer, après une procédure contradictoire, durant laquelle le responsable de traitement incriminé peut présenter des observations orales :
- **une sanction pécuniaire** (sauf pour les traitements de l'État), d'un montant maximal de 150 000 €, et en cas de récidive, jusqu'à 300 000 € ; en cas de mauvaise foi, la CNIL peut ordonner l'insertion de la décision de sanction dans la presse ;
- **une injonction de cesser le traitement** ;
- **un retrait de l'autorisation**.

Par ailleurs, **un arrêt du Conseil d'État du 19 février 2008** a reconnu à la **CNIL** dans l'exercice de son pouvoir de sanction l**a qualité de tribunal**.
Le montant des sanctions pécuniaires susceptibles d'être appliquées peut atteindre 150 000 euros lors du premier manquement constaté et 300 000 euros ou 5 % du chiffre d'affaire hors taxes du dernier exercice s'il s'agit d'une

entreprise dans la limite de 300 000 euros. Le montant de ces sanctions doit en outre ***être « proportionné à la gravité des manquements commis et aux avantages tirés de ce manquement ».***

- La création du « Correspondant Informatique et Liberté » (CIL) le 20 Octobre 2005
(Décret d'application 2005-1309, - Modification du décret de 2005 par le décret 2007-451 du 25 mars 07)
Pour faciliter les missions de la CNIL au niveau « local », le décret du 20 octobre 2005 a créé la fonction de Correspondant informatique et libertés dit « CIL ».
Les CIL (dont la nomination est facultative) sont présents dans différents types d'organisation : les administrations, les associations, les entreprises…
La désignation d'un CIL permet un allégement très important des formalités auprès de la CNIL : exonération de l'obligation de déclaration préalable des traitements ordinaires et courants ; seuls les traitements identifiés comme « sensibles » continueront à faire l'objet de formalités.

Les missions du CIL :
Le correspondant doit, dans le cadre de ses missions :
- Dresser une liste (transmise à la CNIL) des traitements automatisés de l'organisme ne comportant pas de risques manifestes pour les droits et la vie privée des personnes.
- S'assurer que toutes les précautions utiles ont été prises pour préserver la sécurité des données. Il doit donc impérativement être consulté préalablement à la mise en oeuvre de tout nouveau traitement de données.
- Veiller au respect des droits d'accès et d'opposition des personnes concernées par les traitements : il peut ainsi recevoir, gérer, suivre les requêtes et réclamations de celles-ci.
- Porter sur l'information et la formation diffusées aux acteurs des systèmes d'information, pour intégrer les dispositions relatives à la loi et les sensibiliser à ses enjeux.
- Tenir un bilan annuel de ses activités qu'il présente au responsable du traitement et met à la disposition de la CNIL.