

## Chapitre 2 Dans quelle mesure le droit répond-il aux questions posées par le développement du numérique ?

### Compétences :

- Identifier pour l'entreprise les modalités juridiques de protection des actifs immatériels
- Caractériser les conséquences juridiques des choix opérés par l'entreprise sur la protection des personnes, des données
- Qualifier et analyser les clauses de contrats relatives à une vente ou à une prestation de service numérique

### Savoirs associés :

- Le rôle de la CNIL
- La protection des actifs immatériels : droit d'auteurs et droits d'utilisation des services et des applications
- La protection de la personne : les données à caractère personnel, l'identité numérique, l'usage du numérique dans l'activité de travail
- La preuve électronique
- Le contrat de vente électronique
- Le contrat de prestations de service numérique

## **I/ La protection des actifs immatériels**

Le développement des technologies liées à l'univers numérique reste extrêmement rapide. Ces bouleversements technologiques impactent l'économie dans son ensemble, mais également le droit à travers de nouvelles situations à prendre en compte. Si l'adaptation de la sphère juridique n'est pas toujours aussi rapide que l'évolution de ces nouvelles technologies, il n'en demeure pas moins que le droit a su s'adapter en reconnaissant, par exemple, de nouveaux objets juridiques et en leur créant parfois des régimes juridiques spécifiques.

### **A Le nom de domaine**

L'adresse web (URL : Uniform Resource Locator) est reconnue comme un caractère distinctif pour une entreprise.

**Le nom de domaine peut donc être protégé de deux manières :**

– en principe, le nom de domaine s'obtient par une réservation en ligne auprès d'organismes spécialisés. C'est la règle du « premier arrivé, premier servi » qui s'applique. L'utilisation par un tiers d'un nom de domaine déposé permet la mise en œuvre de l'action en **concurrence déloyale**. Fondée sur la responsabilité extracontractuelle (article 1240 du Code civil), elle permet, au détenteur du nom de domaine, d'obtenir des dommages-intérêts pour le préjudice subi. Pour cela, il devra prouver la faute, le dommage et le lien de causalité entre la faute et le dommage.

– le nom de domaine peut aussi être protégé en tant que **marque**. Au sens de la propriété industrielle, la marque est un « signe » servant à distinguer précisément les produits ou services d'une entreprise de ceux de vos concurrents.

Pour pouvoir être protégé en tant que marque, le nom de domaine doit être déposé auprès de l'INPI (Institut national de la propriété industrielle). Ce dépôt permet d'obtenir un monopole d'exploitation sur le territoire français pour 10 ans, renouvelable indéfiniment.

L'utilisation par un tiers de la marque déposée permet la mise en œuvre de l'action en contrefaçon. L'**action en contrefaçon** est ouverte à celui qui est **titulaire d'un droit privatif** sur un signe ou une création (marque, brevet, dessin), auquel il a été porté atteinte. Cette action régie par les dispositions du Code de la propriété intellectuelle peut entraîner **des sanctions pénale et civile** (dédommagement du préjudice subi).

La contrefaçon est, d'une part, un **délit civil** qui se répare par l'octroi de **dommages-intérêts**, et d'autre part, une **infraction pénale** (article L. 335-2 du CPI) qui peut entraîner jusqu'à trois ans de prison et 300 000 euros d'amende.

Lorsqu'il est saisi, le juge vérifie que le droit dont se prévaut le plaignant est valablement protégé, et il statue sur l'atteinte portée à ce droit protégé. La contrefaçon existe du seul fait de l'atteinte au droit privatif, indépendamment de toute faute ou préjudice.

Comme pour les autres signes distinctifs, le nom de domaine ne peut bénéficier d'une protection que s'il renvoie à un site actif. Dans le cas contraire, le juge ne peut vérifier le risque de confusion qui pourrait exister entre le nom de domaine et, par exemple, une marque. Tant que le site est inactif, il ne peut y avoir acte de contrefaçon.

De la même manière, un nom de domaine enregistré préalablement à une marque ne peut constituer un droit antérieur à cette marque s'il n'a pas été exploité. Il faut comprendre ici que la jurisprudence tend à limiter les conséquences de la pratique du cybersquatting ou cybersquattage (il s'agit, pour des tiers, d'enregistrer des noms de domaines qui correspondent à une marque en ayant dès cet enregistrement l'intention de revendre ce nom de domaine au titulaire de la marque). La protection du nom de domaine en tant que marque suppose qu'il soit **licite, distinctif et disponible**.

## **B. Les bases de données**

Les bases de données sont un élément technique essentiel au fonctionnement des systèmes d'information ; elles font partie de ces objets juridiques nouveaux reconnus de manière relativement récente par le droit national.

En effet, la loi du 1er juillet 1998 transposant la directive 96/9 du 11 mars 1996 élabore un régime juridique spécifique pour les bases de données. La loi commence par définir les bases de données (article L. 112-3 du Code de la propriété intellectuelle) comme étant « **un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique, et individuellement accessibles par des moyens électroniques ou par tout autre moyen** ». Le fait que la loi reconnaisse la base de données comme un objet juridique à part entière ne lui retire pas la possibilité d'être également une œuvre de l'esprit protégeable par le droit d'auteur. Ainsi, les bases de données bénéficient d'une double protection : la forme des bases de données est protégée par le droit d'auteur (sous certaines conditions) et le contenu des bases de données bénéficie du droit sui generis ou droit du producteur.

### **1/ La protection par le droit d'auteur**

Si le droit d'auteur demeure un **droit de propriété incorporelle attribué à l'auteur** d'une œuvre de l'esprit, ses composantes ont vu leurs applications s'enrichir. Les deux principales composantes du droit d'auteur sont l'ensemble des **droits moraux** et l'ensemble des **droits patrimoniaux** attribués à l'auteur.

Sont regroupés sous l'appellation « **droits moraux** », les droits de **divulgaration**, de **paternité**, de **retrait et de repentir**, ainsi que le **droit au respect de l'œuvre**. Les intérêts de l'auteur sont protégés perpétuellement et les droits reconnus sont inaliénables et imprescriptibles.

Parallèlement, les droits patrimoniaux regroupent les **droits de représentation, de reproduction, de suite et de destination**. L'application de ces droits peut varier en fonction de l'objet juridique auquel ils sont rattachés.

L'œuvre est protégée depuis sa création jusqu'à 70 ans après la mort de son auteur. Ces droits patrimoniaux ont pour objectif d'organiser une **exclusivité d'exploitation** de l'œuvre au bénéfice soit de l'auteur, soit des intermédiaires qui auraient acquis ou hérité d'une ou de plusieurs de ces composantes. La finalité est ici clairement économique. Pour que l'œuvre soit protégeable, elle se doit de porter l'**empreinte de la personnalité de l'auteur**.

Le droit d'auteur a vocation à s'appliquer sans distinction de genre, de forme d'expression, de mérite ou de destination.

**L'œuvre est protégée dès sa création sans procédure ou déclaration préalable.**

Les enjeux nés de la reconnaissance du droit d'auteur sont majoritairement financiers, le droit d'auteur ou ses composantes patrimoniales deviennent des sources de revenus pour les auteurs dont le maintien semble essentiel pour encourager la création. L'atteinte aux droits d'auteur peut faire l'objet d'une action en contrefaçon.

**L'article L. 335-3 du Code de la propriété intellectuelle définit la contrefaçon** comme toute reproduction, représentation ou diffusion, par quelque moyen que ce soit, d'une œuvre de l'esprit en violation des droits de l'auteur... Ce délit est donc la principale réponse du droit face au non-respect du droit d'auteur.

## **2/ La protection par le droit sui generis**

Le droit sui generis consiste globalement à **donner aux producteurs le droit d'interdire** :

- **l'extraction**, par transfert permanent ou temporaire, de la totalité ou d'une partie qualitativement ou quantitativement substantielle, du contenu d'une base de données sur un autre support, par tout moyen et sous toute forme que ce soit ;
- **la réutilisation**, par la mise à la disposition du public, de la totalité ou d'une partie qualitativement ou quantitativement substantielle, du contenu de la base, quelle qu'en soit la forme.

Néanmoins, pour que le producteur de base de données puisse revendiquer l'application de ce droit sui generis, il doit être en mesure de prouver « **qu'un investissement financier, matériel ou humain substantiel [a] été consacré à sa constitution, sa vérification ou sa présentation** ».

**Cette protection des bases de données commence dès leur création** ou leur **mise à disposition** du public et pour une **durée de 15 ans**. Ce délai sera prolongé d'autant dès lors que les bases de données feront l'objet d'investissements significatifs.

**La structure, l'architecture, d'une base de données peut également être protégée par le droit d'auteur**. Il s'agit ici de protéger la manière dont sont disposées les informations et le choix de celles-ci. Mais, comme pour le droit d'auteur de « droit commun », la protection n'existera que si cette architecture présente un caractère d'originalité suffisant. Cette notion d'originalité est laissée à l'appréciation souveraine des juges. D'une manière générale, l'originalité peut être constatée à travers le choix des matières ou par la disposition des informations.

## **C. Les sites internet**

Il existe deux manières de protéger un site internet :

**1/ la protection du site internet dans son ensemble par le droit d'auteur.** Pour cela, il faut que le site soit **original**.

**L'originalité d'un site internet**, selon la jurisprudence, suppose de démontrer que l'éditeur a réalisé un effort créatif dans la combinaison des éléments qui le composent (rubriques, couleurs, bandeaux, images, texte, etc.) afin de lui conférer « une physionomie propre » et un « parti pris esthétique » portant l'empreinte de la personnalité de l'auteur (Cour d'appel de Rennes, 13 mai 2014) ;

**2/ la protection de chaque élément du site :**

– le site internet peut abriter un certain nombre de **créations graphiques et plastiques** qui peuvent être protégées au titre des **dessins et modèles**. Cette protection fait naître pour leur titulaire un monopole d'exploitation de 5 ans renouvelable quatre fois,

– **le contenu**, les textes du site Internet vont pouvoir être protégés par **le droit d'auteur** s'ils ont le **caractère d'originalité** nécessaire, « **s'ils témoignent de l'empreinte de la personnalité de leur auteur** ». Cette protection existe dès la création de l'œuvre sans formalité administrative particulière (le dépôt n'est pas nécessaire).

## **D. Les logiciels**

**Le logiciel est considéré comme une œuvre de l'esprit et à ce titre fait l'objet d'une protection au titre du droit d'auteur.** La protection de ces éléments nécessite qu'ils soient originaux (effort intellectuel) et concrétisés.

Si le logiciel dans son entier ne fait pas l'objet d'une protection, certains éléments constitutifs du logiciel peuvent être protégés par **le droit d'auteur** :

– **l'interface graphique**, qui permet à l'utilisateur d'interagir avec le programme et qui est reconnaissable par son aspect visuel ;

– **le titre, élément d'identification du logiciel**. Il peut également faire l'objet d'un dépôt de marque ;

– **le manuel d'utilisation** qui explique le fonctionnement du logiciel ;

– **le programme** qui comprend le code source, le code objet...

– **le matériel** de conception préparatoire, soit l'ensemble des travaux ayant contribué à la création du logiciel (prototypes...).

La protection par le droit d'auteur permet **la mise en œuvre de l'action en contrefaçon**.

## **II / L'évolution du droit des obligations**

Le développement du numérique entraîne de nombreuses relations dans les relations contractuelles et au niveau du droit de la preuve. Le droit a donc dû s'adapter et édicter des règles tenant compte des évolutions.

### **A. L'évolution du droit des contrats**

Le numérique permet la conclusion de contrats de vente par voie électronique avec les consommateurs et rend indispensable le recours par les entreprises aux services de prestataires informatiques pour les besoins de leur activité.

#### **1 Les contrats de prestations de service numérique**

Les contrats de prestation de service numérique (hébergement de données, développement de logiciels ou de sites internet, conseils en ingénierie, maintenance matérielle ou logicielle...) se multiplient. La rédaction du contrat de prestation de service numérique s'appuie sur le droit des contrats en général et des contrats de prestation en particulier.

**Les mentions habituelles des contrats** doivent figurer, à savoir l'identification des parties (le nom, la forme juridique, l'immatriculation, adresse, nom du représentant légal...) ; l'objet du contrat avec une description précise des prestations à réaliser ; le prix, le règlement et ses modalités ; les modalités d'exécution de la prestation, les intervenants ; la durée du contrat ; les obligations des parties (prestataire et client) ; les modalités de rupture du contrat ; les modalités de résiliation ; les sanctions en cas de défaut ; la gestion des litiges.

**Les clauses spécifiques du contrat de prestation de service numérique** ont un caractère essentiel surtout s'il est question d'infogérance (création et gestion du site par le partenaire extérieur) :

- **la clause de confidentialité** : le prestataire, qui a accès à de nombreuses informations, s'engage à respecter le secret de l'information, à ne pas la diffuser, à la sécuriser ;
- **les clauses de propriété et de transfert de propriété** : elles permettent de définir qui du prestataire ou du client sera le propriétaire ;
- **la clause de résultat ou la clause de moyens** : l'obligation de résultat impose que le prestataire parvienne au résultat défini dans le contrat alors que l'obligation de moyens engage le prestataire à apporter tous les moyens et toutes ses capacités pour exécuter sa prestation et l'ensemble de ses obligations ;
- **les clauses d'assistance** définissent les conditions d'une assistance téléphonique (horaires, conditions d'accès à une hot line), les tarifs spécifiques applicables, les délais de dépannage...
- **une clause de veille technologique** peut être précisée : le prestataire peut s'engager à rester au courant de l'évolution des solutions informatiques les plus adaptées aux problématiques des clients, et leur en faire part au client.

#### **2 Le contrat de vente par voie électronique**

Un **contrat électronique** est un contrat qui est conclu exclusivement par la voie électronique.

La **validité d'un contrat** repose, selon l'article 1108 du Code civil, sur **trois conditions** :

- le **consentement** des parties **libre, éclairé** ;
- la **capacité des parties contractantes** (les parties doivent être des majeurs capables, c'est-à-dire avoir 18 ans révolus et ne pas être incapables majeurs) ;
- un **contenu licite et certain**.

Pour être **valablement formé**, l'article 1369-5 du Code civil prévoit que le **contrat électronique** doit répondre aux **conditions particulières de la procédure dite « du double-clic »** :

- le consommateur doit pouvoir, avant la conclusion définitive du contrat, vérifier le détail de sa commande (produits, quantité, prix...) et la corriger si cela s'avère nécessaire ;
- le consommateur doit confirmer sa commande ;
- le vendeur doit envoyer un accusé de réception de la commande par voie électronique afin de confirmer à l'acheteur l'achat dans les plus brefs délais.

**Ce n'est qu'après avoir cliqué deux fois (une fois pour commander et une fois pour confirmer sa commande) que le contrat sera formé.**

Dans les faits, cette procédure est matérialisée par une suite d'écrans de saisie validés les uns après les autres par le consommateur. Les textes ne précisent pas le contenu de l'accusé de réception. Il est toutefois évident qu'il doit mentionner les éléments essentiels du contrat qui vient d'être conclu. Toutefois, cet accusé n'a pour objet que de servir de preuve à la conclusion du contrat et n'est pas constitutif de la formation de celui-ci.

**Dans le cadre de ce contrat, les obligations du vendeur sont renforcées :**

- il doit offrir un moyen de paiement sécurisé ;
- il doit s'engager sur la date ou le délai de livraison. Sans mention au contrat, le bien doit être livré ou la prestation exécutée dès la conclusion du contrat. En cas de retard de livraison ou de la prestation, le fournisseur doit en informer le client, qui peut demander à être remboursé dans les 30 jours suivant le paiement. Le remboursement se fait alors en totalité, y compris des frais de réexpédition, si le colis arrive après la rétractation. En cas d'indisponibilité du produit, il doit informer l'acheteur et lui proposer soit de le rembourser, soit de remplacer le produit par un produit équivalent. La loi sur la confiance dans l'économie numérique (LCEN) de 2004 fait peser sur le commerçant une responsabilité de plein droit quant à l'exécution du contrat électronique ;
- le cybercommerçant doit respecter le droit de rétractation (14 jours) du consommateur prévu par l'article L. 121-21 du Code de la consommation. Il doit fournir un formulaire de rétractation.

## **B. L'évolution du droit de la preuve**

Selon l'article 1316-4 du Code civil : « la signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle **manifeste le consentement des parties** aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.

Lorsqu'elle est électronique, elle consiste en **l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache**. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'État ».

Aussi, la preuve électronique doit remplir deux conditions nécessaires à la recevabilité de l'écrit électronique (article 1366 du Code civil) :

- **la personne dont elle émane doit pouvoir être dûment identifiée (grâce à la signature électronique) ;**
- il doit être établi et conservé dans des conditions de nature à en **garantir l'intégrité**.

Une **signature électronique fiable** nécessite donc un **système certifié**, ce qui est très rarement possible dans les échanges de tous les jours.

### **III. La protection des personnes**

L'utilisation des technologies numériques génère des traces qui peuvent être enregistrées et exploitées à des fins commerciales ou à des fins de contrôle. Il est donc nécessaire de mettre en place des mesures juridiques afin de protéger les personnes contre ces risques.

#### **A. La protection de la personne dans la sphère privée (la protection des données personnelles)**

Le 21 juin 2018, la loi sur la protection des données personnelles a été publiée au Journal officiel. Ce texte découle du Règlement général sur la protection des données (RGPD), un règlement européen adopté par le Parlement européen et le Conseil européen depuis le 27 avril 2016. Ce nouveau texte de loi a permis d'adapter la loi informatique et libertés afin de renforcer la protection des données personnelles.

Cette loi s'applique aux traitements automatisés en tout ou partie de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers.

**Selon l'article 2 de la loi :** « 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 ». Sont considérés comme des **données personnelles tous les éléments qui permettent d'identifier une personne** (nom, adresse, numéro d'identification, photo, empreinte...).

Selon le même article : « 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 ».

**Les obligations qui pèsent sur les organisations sont les suivantes :**

– **obligation générale de sécurité et de confidentialité :**

– le responsable du traitement des données doit mettre en œuvre les **mesures de sécurité des locaux et des systèmes d'information** afin de protéger les fichiers et les données contenues dans ces derniers,

– il doit vérifier que **l'objectif de la collecte des données est précis et en accord avec sa finalité**.

Il ne doit d'ailleurs **collecter que les données nécessaires** (principe dit de « minimisation ») à cette finalité. Il doit être capable de démontrer à tout moment qu'il a respecté ce principe,

– il doit vérifier que **l'accès aux données est limité uniquement aux personnes désignées** ou à des tiers qui détiennent une autorisation spéciale et ponctuelle (service des impôts, par exemple),

– il doit fixer une durée **raisonnable de conservation des informations personnelles** ;

– **obligation d'information :**

– l'organisation qui détient des données personnelles doit informer la personne concernée de l'identité du responsable du fichier ; de la finalité du traitement des données ; du caractère obligatoire ou facultatif des réponses ; des droits dont dispose la personne (droit d'accès, de rectification, d'interrogation et d'opposition) ; des transmissions des données,

- l'organisation qui exploite des données personnelles doit respecter les obligations suivantes : recueillir l'accord des personnes dont les données sont collectées ; les informer de leur droit d'accès, de modification et de suppression des informations collectées ; veiller à la sécurité des fichiers et des systèmes d'information ; garantir la confidentialité des données ; indiquer une durée de conservation des données ;
- obligation de mettre en place, pour les traitements de données présentant un risque élevé pour les droits et libertés des personnes (données sensibles comme l'origine, les opinions politiques etc.), une analyse d'impact permettant d'évaluer les risques pesant sur les personnes ;
- obligation de nommer un délégué à la protection des données dont le rôle est d'informer et de conseiller le responsable de traitement et ses employés, de contrôler le respect du règlement européen et du droit français en matière de protection des données ; de conseiller l'organisme sur la réalisation d'une analyse d'impact et d'en vérifier l'exécution ; d'être en contact et coopérer avec l'autorité de contrôle.

### **Les droits des personnes sont renforcés :**

- **elles doivent** donner leur **consentement explicite** à la collecte et au traitement de leurs données ;
- elles ont le **droit à la portabilité des données**. Elles peuvent donc récupérer les données qu'elles ont fournies et les transférer à une autre organisation ;
- elles ont un **droit à l'oubli**. Il est constitué du droit à l'effacement des données et au déréférencement ;
- elles peuvent intenter une action de groupe pour obtenir réparation du préjudice subi suite au non-respect du RGPD par le responsable du traitement.

Ces obligations et ces droits sont garantis par la Commission Nationale Informatique et Libertés (CNIL), organisme indépendant. Dans ce cadre, la **CNIL a pour rôle** :

- **d'informer des personnes des droits** que leur reconnaît la loi ;
- de protéger les droits des personnes ;
- de conseiller et d'accompagner les organisations afin qu'elles soient en conformité avec la loi ;
- de contrôler et sanctionner les organisations qui méconnaissent les dispositions légales. Le montant des sanctions peut s'élever jusqu'à 20 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial.

## **B. La protection de la personne dans la sphère professionnelle**

**Les pouvoirs de l'employeur** lui confèrent le **droit de contrôler le travail** exécuté par les salariés pendant le temps de travail. Toutefois, il est soumis à un certain nombre d'obligations.

### **• Respect des droits et libertés fondamentales des salariés ou principe de proportionnalité**

La surveillance doit être justifiée par la nature du travail à accomplir et être proportionnée au but recherché. Les moyens de surveillance et de contrôle utilisés par l'employeur ne doivent pas porter atteinte aux libertés fondamentales et à la vie privée des salariés. Ainsi, afin de respecter la vie privée du salarié (article 9 code civil) , l'employeur ne peut, sauf cas exceptionnel, ouvrir les courriels, SMS ou dossiers personnels du salarié dès lors qu'ils ont été identifiés comme tels.

### **• Information collective et individuelle des salariés**

L'employeur a l'obligation d'informer le comité social et économique préalablement à leur introduction dans l'entreprise de tous « les moyens ou les techniques permettant un contrôle de l'activité des salariés », même s'il ne leur est pas initialement destiné (art. L. 2312-38 du Code du



travail). C'est le cas, par exemple, de l'installation de caméras ayant pour objet d'éviter les vols de la clientèle.

L'exploitation des informations collectées par l'employeur doit respecter le **principe de loyauté** : seules les informations obtenues par des moyens de contrôle portés à la connaissance des salariés peuvent être utilisées comme moyens de preuve.

En plus de l'obligation **d'information collective** (affichage visible), l'employeur doit donc **prévenir chaque salarié des moyens de contrôle mis en œuvre** (art. L. 1222-4 du Code du travail). Dans ce cadre, les personnes concernées doivent être **informées individuellement** (note de service, charte informatique, avenant au contrat de travail...) :

- de la ou des finalités poursuivies ;
- de la base légale du dispositif ou intérêt légitime de l'employeur ;
- des destinataires des données ;
- de la durée de conservation des données ;
- de la possibilité d'introduire une réclamation auprès de la CNIL ;
- etc.

• **Inscription des différents systèmes de contrôle dans le registre des activités de traitement tenu par l'employeur**

Si l'employeur a désigné un Délégué à la protection des données (DPO), il doit être associé à la mise en œuvre des dispositifs de contrôle.

#### IV/ le rôle de la Commission Nationale Informatique et Liberté

<b>La CNIL est une Autorité Administrative Indépendante</b>	Indépendance de l'organisation qui lui permet d'exercer sans pression ses missions y compris sur les fichiers utilisés par les autorités. Ne reçoit d'instruction d'aucune personne. Le président recrute librement ses collaborateurs.
<b>Missions et pouvoirs de la CNIL</b>	
<b>Informier et conseiller les personnes sur leurs droits</b>	Elle <b>reçoit les réclamations</b> , les pétitions et plaintes relatives à la mise en œuvre des traitements des données personnelles.  Elle contribue à <b>l'élaboration des règles</b> dans son domaine en répondant par des avis, des délibérations et des recommandations aux multiples questions soulevées par le traitement des données à caractère personnel.
<b>Réguler et recenser les fichiers de données personnelles</b>	Elle veille à ce que le traitement des données à caractère personnel soit mis en œuvre conformément à la loi.  Elle autorise (ou non) la création de certains fichiers (données biométriques).  Elle contribue à la formation et à l'émergence délégués à la protection des données Ceux-ci deviennent alors ses interlocuteurs privilégiés.
<b>Ses pouvoirs</b>	
<b>Contrôler</b>	Elle peut effectuer dans les organisations, des contrôles et investigations afin d'apprécier la conformité des traitements informatiques. Le refus ou entrave à ces contrôles, sont sanctionnés.
<b>Sanctionner</b>	Elle peut adresser des avertissements, faire des injonctions (enjoindre un responsable de traitement à modifier son fichier par exemple), prononcer des sanctions pécuniaires. Elle a aussi la possibilité de dénoncer au procureur de la république les infractions à la loi, dont elle a connaissance.

#### V/ L'identité numérique

L'**identité de la personne physique** est composée de données inscrite dans l'état civil (date, lieu de naissance, nom, prénom, filiation) qui permettent de l'individualiser de manière unique.

L'**identité numérique** est composée :

de l'identité **objective données formelles** (coordonnées)

et de l'**identité subjective** composées **des données** informelles (commentaires, notes, billets, photos) des traces que laisse l'individu volontairement ou involontairement et que les systèmes informatiques retiennent et des traces que laissent les autres personnes.

L'identité numérique évolue dans le temps en fonction de ce que l'outil informatique et la mémoire des ordinateurs dit de la personne à un moment T. Il s'agit la des traces numériques laissées par les individus sur Internet.

L'identité numérique est la capacité à utiliser de façon sécurisée les attributs de son identité pour accéder à un ensemble de ressources. Il s'agit pour les individus de pouvoir utiliser de façon sécurisées les attributs de son identité (nom, prénom, date de naissance, adresse) afin d'accéder à des services publics en ligne.