**Introduction : le contexte “informatique et liberté”**

Article 1 de la loi du **6 janvier 1978** : “L’informatique doit être au service de chaque citoyen. 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. “

L’informatique est un formidable outil pour l’entreprise, mais un usage abusif, non contrôlé peut porter atteinte à la vie privée de l’individu voire faire évoluer la société vers une société de surveillance. L’essor des NTIC a renforcé cette possibilité : vidéosurveillance, fichiers informatiques, dans les transports (Navigo), cartes à puces, via Internet, dans les bureaux : être anonyme devient difficile.

En France, les gardes fous législatifs existent contre abus et risques de dérapages.

La loi votée le 21 Décembre 1977 (Journal Officiel du 6 Janvier 1978) a été à l’époque une réponse à la crainte que le développement de l’informatique ne porte atteinte à la vie privée de chacun : au début des années 70, certains projets gouvernementaux de constitution de vastes fichiers nominatifs devant servir à l’adm° allaient dans ce sens :

ex projet Safari (Système automatisé pour les fichiers adm et le répertoire des individus) en 1974 ; ou projet GAMIN en 1975 (Gestion Automatisée de Médecine INfantile).

**28 janvier 1981** : Convention au Conseil de l’Europe pour la protection des personnes à l’égard du traitement automatisé des données à caractère personnel.

La Directive européenne du 24 octobre 1995 a prévu un net assouplissement du système de déclaration préalable et un renforcement du contrôle a postériori.

Les différents pays de l’Union Européenne avaient jusqu’à octobre 1998 pour adapter les lois nationales à la Directive, la France aura été l’une des dernières.

La loi du 6 janvier 1978 a été modifiée par la loi du 6 août 2004, transposition de la Directive Europpéene.

Dans la suite du cours seront vus les changements par rapport à la loi de 1978

# La nouvelle loi

Oralement : partir de la loi de 1978 et faire apparaître les changements.

La loi actuelle dite Informatique et Libertés du 6 janvier 1978 et modifiée par la loi du 6 août 2004 : un certain nombre de nouveaux points apparaissent :

**1. Une nouvelle terminologie**

* + La « donnée nominative » est remplacée par la « donnée à caractère personnel », c'est à dire toute donnée permettant d’identifier directement ou indirectement une personne, notion beaucoup plus vaste, ex oral
  + Le traitement de données à caractère personnel : toute opération portant sur ces données
  + Fichier de données à caractère personnel : ens structuré et stable de données personnelle.

**2. La CNIL (Commission Nationale de l’Informatique et des Libertés)**

C’est une autorité administrative indépendante composée de 17 membres nommés pour 5 ans ou pour la durée de leur mandat : 4 parlementaires, hauts magistrats, personnes reconnues pour leur compétence : ils sont inamovibles (garantie de leur indépendance vis à vis du pouvoir).

La CNIL veille au respect de la loi, protéger la vie privée et les libertés de chacun avec de nouvelles compétences :

* elle a le pouvoir de conseiller, s’informer et d’enregistrer les déclarations de traitements automatisés de données à caractère perso, elle doit informer le public (rapport publié tous les ans) ;
* elle a désormais une mission de contrôle et de vérification que la loi est bien appliquée) peut sanctionner et peut ester en justice ; poss de contrôle et de visite renforcé mais opposabilité du secret prof.
* les sanctions vont de l’avertissement, mise en demeure, demande d’interruption de traitement (max 3 mois), verrouiller certaines données (3 mois max), jusqu’à informer le 1 er Min, introduire une procédure en référé.
* Sanctions pécuniaires possibles (comme ART par ex) , elles se situent entre 150 000 et 300 000 €.
* La CNIL peut agir en F à la dde d’une autre « Cnil » de l’UE

**3. Les nouvelles formalités**

LA CNIL a mis en place des procédures simplifiées de déclaration pour se concentrer sur les traitements à risque.

* Certains traitements ne sont soumis à aucune déclaration :
  + Fichiers personnels : ex agenda électronique
  + Partis po, Eglises, associations, syndicats : fichiers d’adhérents
  + Fichiers de paie du personnel
* S’il existe un « correspondant à la protection des données à caract perso » chargé du respect de la loi dans l’ent et qui pourrait saisir la Cnil : allègement des formalités de déclaration
* Les traitements de données génétiques, sensibles, aux infractions, condamnations, les traitements susceptibles d’exclure une pers du bénéfice d’un droit, les interconnexions de fichiers, les traitements avec utilisation du NIR sont soumis à autorisation de la Cnil.
* Si le traitement concerne la sûreté de l’Etat, avis motivé et publié de la Cnil (recul de la loi par rapport à 1978) où nécessité d’un avis favorable.

Elle rend son avis dans un délai de 2 mois renouvelable une fois sur décision de son président.

La déclaration via Internet est possible : nouveaux formulaires en cours d’élaboration.

Délai de 3 ans pour se conformer à la nouvelle loi.

**4. Le respect des règles liées à l’exploitation des fichiers**

La loi actuelle met en avant la nature des données et la finalité des traitements en fonction du risque d’atteinte à la vie privée ou aux libertés individuelles. Ainsi, la collecte des données doit être loyale et licite, pour des finalités déterminées, importance du droit à l’oubli.

Il est interdit de collecter ou de traiter des données à caract perso faisant apparaître direct ou indirectement les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l’appartenance synd des pers ou relatives à la santé ou à la vie sexuelle de celles-ci,

Sauf si consentement exprès de la personne, nécessité médicale, si appartenance à un syndicat par ex, infos rendues publiques par la personne …

Pour de tels fichiers : demande d’autorisation à la CNIL

Les traitements de données à caract perso relatives aux infractions, condamnations et mesures de sûreté ne peuvent être mis en œuvre que par les autorités compétentes (police, justice) et les personnes morales en rapport avec le Code de la propriété intellectuelle pour protéger le droit d’auteur des auteurs/ayant droit (oralement lié au piratage sur Internet).

Renforcement des obligations incombant aux responsables des traitements :

* Informer la pers de la collecte des données, idem pour les communications électroniques (ex cookies) sauf si pour faciliter la dite communication
* Sauf si concerne la sûreté de l’Etat
* Assurer la sécurité des données
* Notion de sous-traitant : le contrat signé doit faire apparaître l’aspect sécurité, le responsable du traitement n’est pas déchargé de ses responsabilités.

Les transferts de données sont impossibles vers Etats où niveau de protection insuffisant des données personnels et des libertés personnelles sauf si accord de la personne (consentement exprès) ou si transfert nécessaire (vie de la pers, intérêt public, lié à l’exécution d’un contrat, ou décret du Conseil d’Etat).

**5. Les droits de la personne fichée**

La Cnil mettra désormais à la disposition du public la liste des traitements déclarés, leur finalité, le responsable du traitement, les données traitées, les destinataires.

* **Droit à l’information préalable** : la saisie des informations ne peut donc se faire à l’insu de l’intéressé qui doit donc être informé de la collecte des informations qui ne doit pas être frauduleuse ou illicite. Les personnes devront être averties des infos relatives à l’identité du responsable du traitement, finalité du traitement.
* **Droit d’opposition**  : Toute personne a le droit de s’opposer, pour des raisons légitimes, à ce que des informations la concernant fassent l’objet d’un traitement. sauf exception, droit de s’opposer aux transferts des infos à des tiers voire à l’extérieur de l’UE.
* **Droit à l’oubli**  : Les informations ne peuvent être stockées que pour une durée nécessaire au traitement -selon la demande d’avis, ou la déclaration.
* **Droit d’accès :** Toute personne peut obtenir communication des informations la concernant dans un fichier, sur justification de son identité ; et ce auprès des organismes détenteurs des fichiers (**droit d’accès direct**).

Droit d’accès simple : gratuit

Coût de la copie doit être inférieur au coût de reproduction

Dossier médical : droit d’accès devenu direct

* **Droit d’accès indirect :** Si le traitement concerne la sûreté publique, police, défense…, la demande doit passer par la Cnil (vérification par un membre magistrat). Toute ou partie des infos ou aucune information n’est communiquée.

Le droit d’accès a été renforcé : ex les destinataires peuvent demander la logique qui sous-tend le traitement de données mais le responsable du traitement peut s’opposer à trop de demandes par ex (abus).

* **Droit de rectification, mise à jour, d’ajout de données complémentaires, de verrouillage ou d’effacement de données** sur justification d’identité si infos inexactes, équivoques, périmées ou si collecte ou utilisation illégale.

La charge de la preuve revient au responsable du traitement.

**6. Les sanctions pénales**

Le secret des fichiers nominatifs est une obligation légale

La loi du 6 janvier 1978 prévoit des sanctions très sévères en cas de violation du secret des fichiers nominatifs, avec un maximum de 5 ans d’emprisonnement et 300 000 euros d’amende (si le fichier est utilisé à d’autres fins que celles initialement prévues.

Ex : la personne qui procède à un traitement automatisé sans faire les formalités légales encourt une peine d’emprisonnement de 6 mois à 1 an et/ou de 300 à 3000 euros d’amende, et éventlt publication et affichage de la condamnation.

Nouvelle disposition pénale : 1 an de prison et 15 000 € d’amende si entrave à l’action de la CNIL.

# Internet et les données personnelles

67% des sites internet recueillaient des informations nominatives sur les internautes en 2000.

Un site Internet est susceptible de comporter des informations nominatives : ex lors de commandes d’un produit, les salariés d’une entreprise...

Un site Internet comportant des informations nominatives doit être déclaré à la CNIL. Téléchargement possible de la déclaration d’un site web.

* Problème lié à Internet : capture, falsification, détournement de leur finalité sans possibilité de contrôle, les mégabases de données nominatives. Les personnes doivent donc être informées avant la mise sur le site des informations les concernant et prévenues de leur droit d’accès et rectification.
* Problème du publipostage électronique et du spamming, ou de la télécopie et début SMS (voir plus loin) : collecte illicite d’adresses mail par exemple.

Suite à une plainte de la CNIL (boite à spam avait entraîné 5 plaintes), condamnation d’un dirigeant d’une société aspirant les adresses mail et procédant à des envois massifs de mails (motif : collecte déloyale d’infos nominatives) : 3000 € d’amende.

* Problème lié à la conservation des données limitée dans le temps (droit à l’oubli)
* Problème des mouchards (cookies ou autres) : publicité personnalisée : Amazon.com n’accepte pas la désactivation de cookies
* Carte Vitale : réseau Santé Sociale fonctionne en Intranet mais des médecins préfèrent passer par Internet : problème de sécurité.

La CNIL insiste sur les dangers qui menacent les internautes qui peuvent être suivis à la trace (vie privée) : risque de capture d’informations nominatives qui peuvent servir à des bases de données, ex spam.

* Problème de la cybersurveillance des salariés dans l’entreprise et des constitutions de fichiers lors des recrutements (loi du 31/12/92)
* L’e-administration en essor avec la mise en ligne des formulaires administratif cyberadministrés : durée de conservation des info sur les connectants limitée à deux semaines.

**1/11/2000 :** Entrée en vigueur des principes Safe Harbor : accord entre l’UE et le Département d’E au commerce US qui fixe un niveau de protection min des données personnelles pour les ent US qui adhèrent en accord avec la DE d’octobre 1995 qui prévoit possible tout flux de données pers à l’ext dans un pays ayant au moins le même degré de protection. Peu d’entreprise US y ont adhéré, environ 78 fin 2001.

Projet au Congrès US pour une éventuelle législation applicable au secteur commercial.

En 2001, 9 pays d’Europe centrale et orientale ont voté une législation sur la protection des données personnelles, idem au Japon, en cours au Mexique.

# Les interventions actuelles de la CNIL et les débats en cours

**Base : rapport publié en avril 2005**

**Fin 2004** : plus d’un million de fichiers déclarés, statistique non faisable ensuite à cause de la nouvelle loi.

La CNIL souligne son insuffisance de moyens

* La CNIL a été saisie plus de 7500 fois en 2004 le plus souvent à cause du non respect du droit d’opposition (problème des fichiers commerciaux et des méga-bases de données, ex Claritas, Consodata qui parviennent à faire de la segmentation très fine). Oralement liste Orange de FT, liste Stop Robinson e-robinson).

Les secteurs les plus touchés par les plaintes auprès de la CNIL : prospection co, banque, travail, télécommunications.

* La CNIL est de plus en plus saisies par des demandes de droit d’accès indirect pour les fichiers STIC (police), JUDEX (gendarmerie) qui recensent toutes les pers mises en cause dans une infraction (crimes ou délits) dès l’enquête préliminaire ; les victimes apparaissent et peuvent demander à être retirées dès que l’affaire est close : 1970 demandes de vérification en 2004 (+ 70% par rapport à 2003).

Or les erreurs dans ces fichiers sont nombreuses, problème de mise à jour : ex oralement à partir du rapport 2004, page 12

**Remarque** : depuis la loi sur la sécurité intérieure du 18 mars 2003 :

Gendarmes et policiers peuvent accéder aux fichiers les uns des autres.

Ces deux fichiers sont sous le contrôle du procureur de la République.

Problème principal du droit à l’oubli, ces fichiers peuvent être consultées dans le cadre d’une enquête administrative.

* Extension prévue du champ des infractions du fichier judiciaire national automatisé des auteurs d’infractions sexuelles. Pour les empreintes génétiques : délits et menaces d’atteintes aux personnes et aux biens. Un suspect peut être enregistré s’il existe des indices graves et concordants.

**En projet :** l’accord de la personne ne serait plus nécessaire

**Remarque** : les données ne sont effacées du fichier si la personne est mise hors de cause.

* Explosion des traces informatiques : vidéo-surveillance ( loi du 20 janvier 1995 vue en TD), badges, traçabilité des déplacements (ex télépéage, Pass de la RATP, les radars automatiques).

Les téléphones portables (de plus en plus important / localisation) : obligation faite aux opérateurs téléphonique et d’Internet de conserver les données de connexion à des fins de police un an max (CNIL : 3 mois) , télépéage.

* Problème du fichier PREVENTEL des opérateurs téléphonique
* Du développement des listes noires pour les crédits
* Rappel à l’ordre de certaines banques : utilisation du bloc note
* Problème des inscriptions à tort, des défichages tardifs des fichiers centraux de la Banque de France (fichier des surendettés et des interdits bancaires)
* Le Fichier Central des Chèques : la CNIL a épinglé plusieurs établissements de crédit pour inscription abusive sur le fichier au moindre incident pour un retrait de carte bancaire.
* Avis sur le dossier médical personnel qui sera accessible via Internet : la CNIL a demandé des garanties pour préserver la vie privée des individus et la confidentialité des données
* La biométrie : en France (idem au niveau européen), la loi du 24 novembre 2003 généralise le recours aux tech biométriques pour la délivrance des visas et pour le contrôle aux frontières.

Avis défavorable sur l’utilisation de telles tech par les établissements scolaires, les employeurs.

Autorisation pour carte de fidélité Aéroport de Nice (inscription non obligatoire)

* Projet INES : Identité nationale électronique sécurisée

Technologie de reconnaissance biométrique avec une puce dans la CNI : avec Etat civil, 2 empreintes digitales et image faciale numérisée pour deux fichiers nationaux (empreintes digitales et images faciales).

**Origine :** règlement européen du 12/12/04 = nouveaux passeport biométrique avec puce lisible à distance (because EU). Et problème de fraude et d’usurpation d’identité.

Débat avec crainte de le voir utilisé abusivement par l’administration.

* « Did they read it ? » : la CNIL considère que l’utilisation de ce service de suivi du courrier électronique (si le message a été lu, combien de fois, quand, s’il a été retransmis…) est illégal en France car collecte d’infos à l’insu des personnes.

**CONCLUSION :**

Le vote de la nouvelle loi a suscité de nombreuses critiques :

* Le fichier de personnes morales (SACEM)
* Le correspondant dans l’entreprise
* Les fichiers publics désormais publié sans avis favorable de la CNIL mais avis seulement motivé : déjà le cas de la loi sur la sécurité intérieure du 18 mars 2003
* Secret professionnel opposable à la CNIL dans les entreprises mais sans entraver l’action de la CNIL

Attentat du 11 septembre 2001 aux EU : volonté des Etats notamment EU qui n’ont aucune loi sur la protection des données personnel, de surveiller mail, flux d’info circulant sur le Net, téléphone...

Problème de l’équilibre entre sécurité collective et liberté individuelle ; tendance actuelle vers un renforcement de la sécurité collective : voir nouveaux projet de loi pour lutter contre le terrorisme à venir.

|  |
| --- |
| Auteur : [Emmanuelle Barbot](mailto:ebarbot@iut-velizy.uvsq.fr%20%20) - Licence ISDRN | IUT de Vélizy | [UVSQ](http://www.uvsq.fr/)  Création graphique et scénarisation multimédia : [Pôle TICE](http://www.tice.uvsq.fr) - [UVSQ](http://www.uvsq.fr/) |