Alain Bensoussan Avocats
Le droit du numérique et des technologies avancées

TELECOM PARISTECH

COURS

DROIT INFORMATIQUE ET LIBERTES

07 Avril 2015

Sommaire analytique

1. Introduction

1.La loi du 6 janvier 1978[1] relative à l'informatique, aux fichiers et aux libertés (dite loi « Informatique et Libertés »), conçue pour encadrer et contrôler le développement de l'informatique, se présente comme un texte de défense des libertés publiques et de l'intimité de la vie privée des personnes.

- L'article 1er de la loi prévoit ainsi que « l'informatique doit être au service de chaque citoyen (…) elle ne doit porter atteinte ni à l'identité humaine, ni au droit de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».

2.Cette loi a été modifiée par la loi du 6 août 2004[2] relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, afin de transposer en droit interne la directive européenne 95/46/CE du 24 octobre 1995[3] relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

3.Cette directive fait actuellement l'objet d'une révision. En effet, conçue au début des années 1990, il convient de l'adapter aux nouvelles problématiques actuelles et notamment à l'apparition ou la diffusion de technologies comme les puces RFID, l'irruption des réseaux sociaux, la géolocalisation, la vidéosurveillance. En outre, en dépit de cette directive, la protection des données à caractère personnel est de plus en plus fragmentée au sein de l'Union créant une insécurité juridique et pratique pour les acteurs.

4.Dans le cadre cette révision, la Commission européenne a adopté le 25 janvier 2012 une proposition de règlement européen destiné à réviser le cadre de la protection des données personnelles[4]. Le 13 janvier 2013 le Parlement Européen a publié un projet de résolution législative sur ladite proposition de règlement[5].

5.Les nouveautés de la proposition de règlement du 25 janvier 2012 sont notamment les suivantes :

- les procédures et modalités d'exercice des droits des personnes, ainsi que les informations à communiquer en cas de demande d'exercice de son droit d'accès par une personne concernée ;
- la clarification des conditions de recueil du consentement au traitement de ses données personnelles par la personne concernée ;
- détermination de l'autorité compétente sur la base du critère de l'établissement principal du responsable de traitement ;
- la consécration du droit à l'oubli pour les citoyens ;
- possibilité de procéder à certains transferts hors de l'Union européenne par les responsables de traitement sur la base d'une auto-évaluation des conditions de sécurité des échanges;

[1] Loi n°78-17 du 6-1-1978 relative à l'informatique, aux fichiers et aux libertés, JO du 7-1-1978.
[2] Loi n°2004-801 du 6-8-2004 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 6-1-1978 relative à l'informatique, aux fichiers et aux libertés, JO du 7-8-2004.
[3] Dir. n°95/46/CE du Parlement européen et du Conseil du 24-10-1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JOCE (L) 281 du 23-10-1995.
[4] Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données personnelles et à la libre circulation de ces données (règlement général sur la protection des données).
[5] Projet de rapport sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données 2012/0011(COD)

- principe de transparence pour le traitement des données ;
- une responsabilité globale du responsable de traitement ;
- le responsable de traitement doit informer la personne concernée sur la durée de conservation, le droit d'introduire une réclamation, les transferts internationaux et la source des données ;
- le droit à la portabilité des données ;
- l'obligation, pour les responsables du traitement et les sous-traitants, de conserver une trace documentaire des opérations de traitement sous leur responsabilité ;
- l'obligation de mettre en place une évaluation des risques présentés par les traitements de données à caractère personnel et implémenter les mesures techniques et organisationnelles de sécurité appropriées au regard des règles de l'art et de leur coût ;
- l'obligation, pour les responsables du traitement et les sous-traitants, d'effectuer une analyse d'impact relative à la protection des données préalablement aux traitements présentant des risques
- le renforcement des obligations en matière de sécurité et de confidentialité et notamment l'obligation de notifier les violations de sécurité aux autorités compétentes;
- l'obligation de désigner un délégué à la protection des données dans certains cas ;
- instauration de règles en matière de coopération ;
- le renforcement des sanctions pouvant être prononcées par les autorités de protection des données.

6.La proposition de règlement européen a également modifiée certaines notions :

- la définition de « données à caractère personnel » a été élargie répondant à la simple définition de «toute informations se rapportant à une personne concernée »
- La définition de « fichier » a également été élargie, le critère de stabilité ayant été supprimé.
- Les définitions du responsable du traitement et du destinataire ont évolué.
- Les conditions du droit d'opposition ont été modifiées. L'article 38 de la loi de 1978 prévoyait un droit d'opposition pour « motifs légitimes » alors que l'article 39 de la proposition de règlement soumet le droit d'opposition à des « raisons tenant d'une situation particulières ».

7.La Commission des libertés civiles, de la justice et des affaires intérieures (LIBE) a adopté le 21 octobre sa position au sujet de la proposition de règlement européen sur la protection des données[6].

8.Les députés européens ont notamment introduit :

- Des sauvegardes pour les transferts de données aux pays tiers ;
- L'obligation d'avoir un consentement explicite ;
- Le droit à l'effacement ;
- Des amendes plus élevées pour les entreprises violant les règles (allant jusqu'à 100 millions d'euros ou 5% du chiffre d'affaires).

9.Il apparait au regard de ces nouveautés et modifications susmentionnées que la proposition de règlement tend en faveur d'une protection renforcée des données personnelles s'inscrivant dans la lignée de la politique de l'Union Européenne qui a érigé ces dernières années la protection des données personnelles comme un droit fondamental intrinsèque et non plus comme un vecteur du droit à la vie privée.

10.L'article 8 de la Charte des droits fondamentaux de l'Union européenne et l'article 16 du traité sur le fonctionnement de l'Union Européenne prévoient ainsi que :
- « Toute personne a droit à la protection des données à caractère personnel la concernant ».

[6]<http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2012)0011_/com_com(2012)0011_fr.pdf>

11.Une fois le règlement adopté, les responsables de traitement auront un délai de deux ans pour se mettre en conformité.

12.La loi « Informatique et libertés » modifiée conserve l'intitulé choisi par le législateur en 1978, à savoir, la loi relative à l'informatique, aux fichiers et aux libertés.

13.Or, la réglementation des communications électroniques n'est pas sans soulever certaines questions à caractère « sensible ». Ainsi, en est-il des données à caractère personnel (« données personnelles ») qui transitent par la voie des communications électroniques et pour lesquelles il faut concilier les intérêts économiques (liberté de circulation de l'information) et la protection de la vie privée.

14.Les dispositions de la loi Informatique et libertés modifiée trouvent donc un domaine d'application en matière de communications électroniques.

15.Avant d'aborder les obligations, les droits et les différentes procédures que la loi Informatique et libertés impose, il sera étudié la Commission nationale de l'informatique et des libertés[7] (Cnil), que la loi de 1978 a mise en place pour l'application des dispositions qu'elle prévoit.

16.Le législateur a, en effet, voulu se doter d'un outil particulier en confiant à la Cnil une mission définie de façon très large, puisqu'elle concerne aussi bien l'information des personnes sur leurs droits que le contrôle des applications informatiques lors du traitement des données personnelles.

2. Les missions et les pouvoirs de la Cnil

17.La Cnil, autorité administrative indépendante, peut affirmer son autorité grâce à toute une gamme de missions et de pouvoirs qui lui permettent de suivre les développements de l'informatique et de l'encadrer avec des moyens adaptés à chaque circonstance particulière.

18.Ses modalités de fonctionnement sont fixées à la fois par la loi Informatique et libertés modifiée, le décret d'application de la loi informatique et liberté du 20 octobre 2005 modifiée par le décret du 25 mars 2007 pris en Conseil d'Etat et le règlement intérieur de la Commission.

2.1 Les missions d'information

2.1.1 Les actions générales

19.La mission d'information de la Cnil est une mission qui implique une réciprocité.

20.Tout d'abord, la Cnil doit se tenir « informée de l'évolution des technologies de l'information » et, le cas échéant, rendre public son appréciation des conséquences qui en résultent pour l'exercice des droits et libertés[8].

21.Au sein de la Commission, le service informatique est plus particulièrement chargé de se tenir informé des développements de l'informatique. Cette nécessité d'information, qui constitue une importante obligation de la Commission, paraît essentielle pour que celle-ci encadre réellement le développement de l'informatique.

[7] Chapitre 3 de la loi Informatique et libertés modifiée.
[8] Art. 11, 4° de la loi Informatique et libertés modifiée.

22.A l'inverse, la Cnil se doit d'informer le public sur la loi Informatique et libertés modifiée et sur ses modalités d'application. Ses principales missions d'information sont définies de la façon suivante :

- informer toutes les personnes concernées et tous les responsables de traitements de leurs droits et obligations[9] ;

- tenir à jour et mettre à la disposition du public la liste des traitements automatisés ayant fait l'objet de formalités préalables avec leurs principales caractéristiques[10], ainsi que ses avis, décisions ou recommandations[11] ;

- présenter chaque année, au président de la République, au premier ministre et au Parlement un rapport public qui rend compte de l'exécution de sa mission[12] ; ce rapport, qui décrit les procédures et les méthodes de travail de la Cnil, est publié par la documentation française.

23.En plus de ses missions légales d'information, la Cnil a pris, de sa propre autorité, différentes mesures afin de faciliter l'information des personnes ; elle met notamment à la disposition du public un site internet « www.cnil.fr » ainsi qu'un service « allô Cnil » (01 53 73 22 22).

24.Elle a également constitué un centre de documentation accessible au public et tient à la disposition de ce même public la liste thématique de ses principales délibérations (site « www.legifrance.gouv.fr »).

25.Enfin, la Cnil participe à différents salons, ainsi qu'à différentes réunions de concertation avec les professionnels et le public.

2.1.2 Les conseils et recommandations

26.La Cnil complète sa mission d'information par l'édiction de propositions de conseils ou de recommandations qui ont pour objectif d'orienter ou d'influer l'action des personnes. Traditionnellement, la Commission s'adresse directement aux pouvoirs publics.

27.A la demande d'organisations professionnelles ou d'institutions regroupant principalement des responsables de traitement, elle donne un avis sur la conformité des projets de règles professionnelles et des produits et procédures, sur les garanties offertes par les règles professionnelles et délivre les labels (possibilité de faire appel à des personnes extérieures indépendantes pour procéder à l'évaluation[13]).

[9] Art. 11, 1° de la loi Informatique et libertés modifiée. Ce principe de publicité connaît une seule exception posée par l'article 31 de la loi Informatique et libertés modifiée qui concerne les traitements intéressants la sûreté de l'Etat, la défense et la sécurité publique, ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales, ou l'exécution de condamnations pénales ou de mesures de sûreté.
[10] Art. 3, I de la loi Informatique et libertés modifiée.
[11] Art. 31, II de la loi Informatique et libertés modifiée.
[12] Art. 11, 4° dernière phrase.
[13] Loi n° 2009-526 du 12-5-2009 de simplification et de clarification du droit et d'allègement des procédures (Art. 104, 105 et 106)

28.La Commission répond aux demandes d'avis des pouvoirs publics et des juridictions. Ainsi, la Cnil a rendu public l'avis rendu à propos de la LOPPSI 2 « projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure »[14].

29.Ses conseils interviennent le plus souvent suite à la demande d'une personne particulière ou d'un déclarant en ce qui concerne l'interprétation d'un point particulier de la loi ou la mise en œuvre, parfois à titre d'expérimentation, d'un traitement automatisé.

30.La demande de conseil constitue, en réalité, un moyen de consulter la Cnil avant toute élaboration d'un nouveau procédé ou d'une nouvelle technologie informatique. Elle permet de régler, au préalable, toutes les difficultés juridiques qui auraient des conséquences techniques importantes sur le système élaboré.

31.Si les conseils n'ont pas de valeur juridique, il paraît cependant certain qu'un déclarant qui aurait préalablement interrogé la Commission peut difficilement, lors de sa demande d'avis ou de sa déclaration, présenter un dossier très différent des conseils qui lui ont été donnés.

32.Les recommandations de la Cnil prennent la forme d'une délibération expresse. Le Conseil d'Etat, qui s'est prononcé sur la nature juridique des recommandations, considère qu'il ne s'agit pas de textes ayant une valeur impérative[15], échappant ainsi au contrôle juridictionnel de légalité. Toutefois, la Cnil considère que ses propres recommandations emportent une valeur indicative très forte.

2.2 Les missions de contrôle

33.La Cnil a une mission générale de veiller à ce que les traitements soient mis en œuvre conformément aux dispositions de la loi[16].

34.Sur les fondements des articles 11-2 f) et 44, la Commission dispose d'un pouvoir général de contrôle sur tout traitement entrant dans le champ d'application de la loi.

35.En pratique, la Cnil charge, par décision particulière, un ou plusieurs de ses membres ou de ses agents de missions de vérification des conditions de mise en œuvre d'un traitement[17].

36.En tout état de cause, lorsqu'elle effectue un contrôle sur place, la Cnil s'intéresse aussi bien aux traitements automatisés qu'aux informations conservées sur d'autres supports.

37.Si la loi ne le prévoit pas expressément, la Commission considère que compte tenu de la mission générale qui lui est confiée, elle dispose d'un pouvoir d'auto-saisine. Elle peut donc, en toute liberté, décider de la réalisation d'un contrôle.

38.Dans la plupart du temps cependant, ce contrôle est la conséquence d'une réclamation, d'une plainte ou d'une pétition adressée à la Commission, d'une campagne de presse ou de l'instruction d'un dossier de déclaration à la Cnil qui fait apparaître des problèmes sensibles de son point de vue.

[14] Cnil, Délib. n°2009-200 du 16-4-2009 portant avis sur sept articles du projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure ; Note d'observation de la cnil relative à certaines dispositions du projet de loi d'orientation et de programmation de la performance de la sécurité intérieure (Loppsi 2), 6-5-2010.
[15] CE cont. 27-9-1989 n°74548 74549 74550.
[16] Art. 11, 2° de la loi Informatique et libertés.
[17] Art. 44, I de la loi Informatique et libertés modifiée.

2.2.1 Les modalités du contrôle

39.Le contrôle s'effectue après l'information préalable du procureur de la République territorialement compétent.

40.Les membres de la Commission et les agents de ses services habilités peuvent se faire communiquer tout document nécessaire à l'accomplissement de leur mission[18], recueillir sur place ou sur convocation tout renseignement et toute justification utile. Ils peuvent accéder aux programmes informatiques et aux données.

41.En cas d'opposition du responsable des lieux, la Commission peut être autorisée par l'autorité judiciaire à effectuer la visite[19].

42. Pour que cette opposition puisse être valablement exercée, le Conseil d'Etat a précisé que :

> « toutefois, la faculté du responsable des locaux de s'opposer à la visite, laquelle ne peut alors avoir lieu qu'avec l'autorisation préalable du juge ; qu'une telle garantie ne présente néanmoins un caractère effectif que si le responsable des locaux ou le représentant qu'il a désigné à cette fin a été préalablement informé de son droit de s'opposer à la visite et mis à même de l'exercer ».

43.Dans différentes affaires[20], le responsable n'avait pas été informé de son droit de s'opposer à la visite des membres de la commission. Dès lors, le Conseil d'Etat a considéré que la procédure devait être considérée comme irrégulière, et les sanctions prises par la Cnil sur la base des informations collectées annulées.

44.La Cnil a pris acte de ces décisions et procède dorénavant systématiquement à l'information des personnes faisant l'objet d'un contrôle sur place de l'ensemble des éléments prévus à l'article 44 de la loi et notamment :

- de leur droit à s'opposer à ce contrôle ;
- dans cette hypothèse, de la possibilité pour le président de la Cnil de saisir le président du tribunal de grande instance compétent afin que celui-ci autorise, par ordonnance, la mission de contrôle, y compris en faisant appel à la force publique.

45.En pratique, la mission est réalisée en conformité avec les règles de procédure résultant du règlement intérieur de la Cnil.

46.La visite fait alors l'objet d'un rapport signé par le membre ou agent de la Commission qui y a procédé.

47.Ce rapport est communiqué à la personne concernée qui est informée qu'elle dispose d'un certain délai à compter de la réception de ce rapport pour faire connaître ses observations et demander à être entendue, assistée ou non d'un conseil, par la Commission.

48.La Cnil peut décider, à tout moment, de contrôler des traitements de données personnelles.

49.Ce contrôle peut intervenir a priori, c'est-à-dire à l'occasion d'une demande de conseils ou de déclaration à la Commission. Il peut également être effectué a posteriori après que le traitement ait

[18] Art. 44, III de la loi Informatique et libertés modifiée.
[19] Art. 44, II de la loi Informatique et libertés modifiée.
[20] Notamment : CE cont. 6-11-2009 n° 304300 ; CE cont. 6-11-2009, n° 304301 ; CE 7-7-2010 n° 309731, 10e et 9e sections réunies.

été déclaré, lorsque la Commission considère qu'elle a suffisamment d'éléments nouveaux pour aller vérifier sur place la mise en œuvre du traitement.

50.Le contrôle peut également être décidé à la suite d'une pétition, d'une réclamation ou d'une plainte pour un traitement qui ne paraît pas remplir les obligations légales.

51.La décision de contrôle peut être prise pour effectuer le bilan de la mise en œuvre d'un traitement particulièrement sensible aux yeux de la Commission.

2.2.2 Les conséquences du contrôle

52.La Cnil considère qu'elle dispose d'un large pouvoir d'appréciation quant aux suites données au contrôle. Ce pouvoir peut aller du classement de l'affaire à la suite du contrôle jusqu'à l'avertissement de la Cnil ou la transmission au parquet des éléments en sa possession.

53.Dans la plupart des cas, il suffit que l'autorité concernée obtempère aux remarques et prescriptions de la Cnil pour que celle-ci prenne acte par délibération des modifications intervenues et procède au classement du dossier.

54.Dans d'autres cas, s'ils sont considérés plus sérieux par la Commission quant au non respect de la loi, la Cnil adresse un avertissement qui, parfois, est qualifié d'avertissement solennel. L'objet de cet avertissement est surtout d'assurer une certaine publicité aux manquements constatés de façon à obtenir un effet dissuasif.

55.Dans les cas les plus graves, qui correspondent en pratique à des hypothèses non résolues par une concertation entre la Cnil et l'organisme concerné, la Commission décide de transmettre au parquet les infractions dont elle a connaissance. Le pouvoir d'appréciation de la Commission quant à la transmission au parquet est très critiqué par une partie de la doctrine qui considère qu'en application de l'article 40 du Code de procédure pénale, la Cnil comme toute autre autorité publique n'a pas de pouvoir d'appréciation en la matière.

56.Enfin, la Cnil doit informer les auteurs de réclamations, pétitions et plaintes des suites données à leurs demandes[21].

57.Le refus de la Cnil de donner suite à une plainte déposée auprès d'elle par un particulier est constitutif d'un excès de pouvoir susceptible de faire l'objet d'un recours.

58.Le délit d'entrave à l'action de la Cnil est puni d'un an d'emprisonnement et de 15.000 euros d'amende[22]. Les actes constitutifs de ce délit sont :

- l'opposition à l'exercice de vérification sur place lorsque la visite a été autorisée par le juge ;
- le refus de communiquer les renseignements et documents utiles, leur dissimulation ou disparition ;
- la communication d'informations non conformes au contenu des enregistrements ou qui ne présentent pas ce contenu sous forme directement accessible.

[21] Art. 11, 2°c de la loi Informatique et libertés modifiée.
[22] Art. 51 de la loi Informatique et libertés modifiée.

59.Cependant, la Cnil a souligné la difficulté d'articulation entre le délit d'entrave à son action et l'obligation d'information du responsable de traitement sur la possibilité de s'opposer à un contrôle sur place mise à sa charge par la jurisprudence.

2.3 Les pouvoirs règlementaires

60.La loi Informatique et libertés modifiée confère à la Cnil un pouvoir général de prendre des décisions réglementaires. Ce pouvoir réglementaire est strictement limité à :

- l'établissement du règlement intérieur de la Commission : ce règlement intérieur[23] a été élaboré en 1987 et modifié par des délibérations ultérieures; il permet de préciser les modalités d'intervention de la Cnil dans l'exercice de la plénitude de ses missions. La délibération n°2006-147 du 23 mai 2006 fixe le règlement intérieur de la Cnil. Cette délibération a été modifiée par deux délibérations respectivement des 8 septembre et 10 novembre 2011 relatives à la procédure de labellisation.
  La loi du 12 mai 2009 portant simplification et clarification du droit et allègement des procédures, prévoit en effet que le règlement intérieur de la Cnil doit prévoir les modalités de mise en œuvres de la procédure de labellisation[24] ;

- l'édiction de normes simplifiées[25] : la Commission établit des textes réglementaires généraux pour les catégories les plus courantes de traitements de données personnelles, dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés[26]. C'est donc la Cnil qui, de sa propre autorité, apprécie si certains types de traitements peuvent faire l'objet d'une norme simplifiée. Sur le plan pratique, la Commission a adopté à ce jour plus de 50 normes simplifiées ;

- l'édiction de règlements types[27] en vue d'assurer la sécurité des systèmes. Si la Cnil a effectivement adopté en 1981 une recommandation en matière de sécurité[28], elle s'est, jusqu'à ce jour, refusée à utiliser son pouvoir d'édicter des règlements types pour assurer la sécurité et la confidentialité des systèmes d'information.

61.Il semble que la Commission considère que, compte tenu de l'évolution technique rapide de l'informatique, il apparaît difficile d'imposer aujourd'hui des prescriptions quant à la sécurité qui seraient très rapidement dépassées technologiquement.

2.4 Le pouvoir de sanctions administratives

62.Depuis la réforme de la loi Informatique et libertés en août 2004, la Cnil dispose également du pouvoir particulier de prononcer des sanctions administratives.

63.Face à l'accroissement de ce pouvoir de sanction, le Conseil d'Etat a considéré que la Cnil devait être qualifié de tribunal au sens de l'article 6-1 de la Convention européenne de sauvegarde des

[23] Art. 13 II de la loi Informatique et libertés modifiée.
[24] Art. 13 II dernier alinéa de la loi Informatique et libertés modifiée.
[25] Art. 11, 2°b de la loi Informatique et libertés modifiée.
[26] Art. 24 de la loi Informatique et libertés modifiée.
[27] Art. 11, 2°b de la loi Informatique et libertés modifiée.
[28] Cnil, Délib. n°81-94 du 21-7-1981 portant adoption d'une recommandation relative aux mesures générales de sécurité des systèmes d'information.

droits de l'homme et des libertés fondamentales. Cette décision a notamment pour conséquence d'imposer à la Cnil le respect des principes d'impartialité et d'équité.

64.Dans les cas graves d'une inobservation de la loi, la Commission peut adresser au responsable du traitement un avertissement et le mettre en demeure de faire cesser le manquement dans un délai qu'elle fixe[29].

65.Lorsque le responsable du traitement fait cas de mauvaise foi, la Commission peut rendre publics les avertissements et les sanctions qu'elle prononce dans des publications, journaux ou supports qu'elle désigne.

66.La Cnil peut aussi prononcer une injonction de faire cesser le traitement si le responsable ne se conforme pas à la mise en demeure.

67.Elle a également la possibilité de prononcer des sanctions pécuniaires, proportionnées à la gravité des manquements commis ou aux avantages tirés du manquement[30]. Ces sanctions peuvent atteindre 150.000 à 300.000 euros selon les cas.

68.A titre d'exemple, la CNIL vient de prononcer le 3 janvier 2014 une sanction pécuniaire d'un montant de 150 000 euros à l'encontre Google Inc. Pour défaut d'information, non définition d'une durée de conservation, défaut de base légale pour la combinaison des données et défaut de recueil du consentement[31].

69.En cas d'urgence, lorsque la mise en œuvre du traitement entraîne une violation des droits et libertés mentionnés à l'article premier de la loi, elle peut décider l'interruption du traitement ou le verrouillage des données traitées[32].

70.Enfin, en cas d'atteinte grave et immédiate aux droits et libertés mentionnés à l'article premier de la loi, le président de la Cnil peut demander, par la voie du référé, à la juridiction compétente d'ordonner, le cas échéant sous astreinte, toute mesure de sécurité nécessaire à la sauvegarde de ses droits et libertés[33].

71.Les sanctions sont motivées et notifiées au responsable du traitement sur la base d'un rapport contradictoire. Elles peuvent faire l'objet d'un recours de pleine juridiction devant le Conseil d'Etat[34].

2.5 La situation de la CNIL en 2012

72.En 2012, la Cnil a renforcé ses contrôles et connu un nombre record de plaintes. Elle a ainsi effectué plus de 458 contrôles ce qui représente 19% de plus qu'en 2011, et a reçu 6017 plaintes soit une augmentation de 4.9% par rapport à 2011. La Cnil a également prononcé 43 mises en demeure et 4 sanctions financières.

[29] Art. 45, I de la loi Informatique et libertés modifiée.
[30] Art. 47 de la loi Informatique et libertés modifiée.
[31] Cnil, Délib. n°2013-420 du 03-01-2014 prononçant une sanction pécuniaire à l'encontre de la société Google Inc.
[32] Art. 45, II de la loi informatique et libertés modifiée.
[33] Art. 45, III de la loi Informatique et libertés modifiée.
[34] Art. 46, al. 3 de la loi Informatique et libertés modifiée.

3. Le champ d'application de la loi

La présente partie aura trait au champ d'application de la loi du 6 janvier 1978 telle que modifiée par la loi n°2004-801 du 6 aout 2004.

3.1 Les données personnelles

3.1.1 Une information relative à une personne physique

73.La loi Informatique et libertés modifiée s'applique aux « données à caractère personnel » concernant les personnes physiques. Ces données sont définies comme étant :

74. « 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[35] ».

75.Sur ce point, la loi s'inscrit dans la continuité de la directive européenne 95/46/CE. La Cnil interprète de façon très extensive la notion de données personnelles : dès lors que les données permettent de remonter à la personne concernée et qu'il reste une possibilité d'identifier à qui ces données s'appliquent, celles-ci sont considérées comme ayant un caractère personnel.

76.A titre d'exemple, la donnée personnelle peut concerner un patronyme, un numéro de sécurité sociale, un numéro d'immatriculation d'un véhicule automobile, photo, adresse e-mail et, plus généralement, toutes données qui, sans avoir un rapport direct (nom, prénom, adresse…), permettent d'établir un lien avec la personne physique concernée.

77.La définition de la donnée personnelle ne se référant qu'à la personne physique, la législation ne protège donc pas les personnes morales. Cette question a été débattue en deuxième lecture devant l'Assemblée Nationale qui a finalement considéré que le droit d'accès à des informations concernant des personnes morales risquait de donner lieu à des violations du secret professionnel et commercial.

78.Toutefois, la Cnil a déjà eu l'occasion d'appliquer certaines dispositions de la loi Informatique et libertés aux personnes morales. Dans une délibération de juillet 1984[36], elle a estimé que « si le droit d'accès à un caractère strictement individuel, il convient d'en reconnaître l'exercice aux personnes physiques, représentants légaux des entreprises dès lors que le nom de ces personnes figurent dans le fichier en tant que dirigeants, actionnaires ou associés ».

3.1.2 L'identification de la personne physique

79.La loi informatique et libertés modifiée précise que :

80.« Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auquel peut avoir accès le responsable du traitement ou toute autre personne[37] ».

81.Constituent des informations propres à la personne celles relatives à son état civil (nom, prénom, sexe, date et lieu de naissance, adresse, etc.) ainsi que toutes celles relatives à ses caractéristiques

[35] Art. 2, al. 2 de la loi Informatique et libertés modifiée.
[36] Cnil, Délib. n° 84-28 du 3-7-1984, extrait du 5ème rapport d'activité de la Cnil.
[37] Art. 2, al. 2 de la loi Informatique et libertés modifiée.

physiques (image, voix, empreintes digitales ou génétiques), sociales ou économiques, dès lors que la personne concernée est directement reconnaissable.

82.Sont également des données personnelles les images des personnes permettant, au moins indirectement, par rapprochement avec d'autres critères, l'identification des personnes dont l'image a été captée par la caméra d'un système de vidéosurveillance[38].

83.La loi du 21 janvier 1995, dite loi Pasqua, a expressément retiré la vidéosurveillance du champ d'application de la loi Informatique et libertés. Les enregistrements visuels de vidéosurveillance ne sont considérés comme des données personnelles au sens de la loi Informatique et libertés modifiée que s'ils sont utilisés pour la constitution d'un traitement de données à caractère personnel[39].

84. Certaines dispositions de la loi du 21 janvier 1995 ont été modifiées par la loi LOPPSI 2 du 14 mars 2011.

85.Les nouvelles dispositions visent notamment à étendre les finalités pour lesquelles le recours à la vidéosurveillance de voie publique peut être autorisé. Ces nouvelles finalités concernent :

- la régulation des flux de transport ;
- la prévention de lieux particulièrement exposés au trafic de stupéfiants ou de trafics illicites ;
- la prévention des risques naturels ou technologiques.

86.Par ailleurs, le texte offre la possibilité aux autorités publiques, après information préalable du maire, de déléguer l'exploitation de leur système de vidéoprotection à des opérateurs publics ou privés agissant pour leur compte, sur la base d'une convention type agréée par le Préfet.

87.Une telle délégation étant susceptible de porter atteinte à l'intégrité du processus en termes de fiabilité et de sécurité, l'article 10 de la loi du 21 janvier 1995 modifiée par la LOPPSI 2 prévoit que le contrôle des dispositifs de vidéosurveillance de voie publique et des lieux ouverts au public sera confié aux commissions départementales mais aussi à la Cnil, qui l'exerçait déjà pour les lieux privés et pour les dispositifs combinés à des traitements automatisés de données.

88.Est réputée indirectement personnelle et entre donc dans le champ d'application de la loi Informatique et libertés modifiée une donnée codée qui peut être reliée soit explicitement par une table correspondante ou par un algorithme, soit implicitement par un ensemble de critères combinés (âge, sexe, fonction etc.) permettant au sein d'une population donnée, de rendre identifiable la personne concernée.

89.Peu importe que l'identification soit possible par le responsable du traitement ou par un tiers. Constituent ainsi des données personnelles les numéros de téléphone, les plaquettes d'immatriculation des véhicules, les trois premières lettres du nom patronymique associées à un numéro de dossier papier, le numéro du badge et autres cas, dès lors qu'une possibilité d'identification existe.

90.Le numéro de carte bancaire doit également être considéré comme une donnée indirectement personnelle.

[38] Cnil, Délib. n° 94-56 du 21-6-1994, 15ème rapport d'activité de la Cnil, p. 85.
[39] Art. 10, 1° de la loi n° 95-73 du 21-1-1995 d'orientation et de programmation relative à la sécurité, JO du 24-1-1995.

91.Enfin, l'adresse électronique constitue une donnée personnelle[40].

92.Par contre, les constatations visuelles et la collecte d'adresses IP effectuées par un agent assermenté, dans le cadre des constatations prévues à l'article L.331-2 du code de la propriété intellectuelle, ne constituent pas un traitement de données à caractère personnel[41].

3.2 Les traitements

3.2.1 Les traitements automatisés

93.La loi Informatique et libertés modifiée se préoccupe de la notion de « traitement de données à caractère personnel ».

94.Cette notion, qui va bien au-delà de la notion de fichier, désigne :

95. « 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[42] ».

96.Le responsable du traitement est alors désigné comme la personne, l'autorité publique, le service ou l'organisme qui détermine les finalités et les moyens du traitement[43].

97.Dès 1979, la Cnil a précisé qu'un traitement automatisé ne se limite pas à la notion de fichier au sens strict. Selon la Commission, la notion de traitement correspond à l'ensemble des informations (fichier) et des logiciels qui concourent à la mise en œuvre d'une fonction principale donnée. Par exemple, un tri ou une simple sélection effectuée de façon automatique à partir d'un ou plusieurs fichiers d'adresses constituent un traitement automatisé.

98.La jurisprudence fait également une large interprétation de la notion de traitement.

99.Elle considère que le traitement de données personnelles n'est pas constitué par la réunion de toutes les phases, depuis la collecte jusqu'à la destruction des données, mais comme l'ensemble des calculs et manipulations informatiques mis en œuvre à chacun des moments de l'élaboration et de l'exploitation des fichiers[44].

100.En outre, les simples saisies et collecte automatisée d'informations constituent un traitement, même si aucune utilisation n'est encore faite. Ainsi, un traitement automatisé peut n'être constitué que par l'un des éléments constitutifs de la notion de traitement, par la seule collecte ou l'enregistrement des données personnelles.

101.La définition extensive de la notion de traitement permet d'appliquer la loi Informatique et libertés modifiée à tout nouveau procédé automatisé, quelle que soit la nature du support ou la technique utilisée, dès lors que les données recueillies sont destinées à être contenues ou appelées à figurer dans des fichiers.

[40] Cnil, Délib. n° 99-048 du 14-10-1999 portant adoption du rapport relatif au publipostage électronique et à la protection des données personnelles.
[41] Cass. crim. 19-1-2009 n° 08-84.088.
[42] Art. 2, al. 3 de la loi Informatique et libertés modifiée.
[43] Art. 3, I de la loi Informatique et libertés modifiée.
[44] TGI Paris, 17ème ch. 5-12-1995 : Expertise, mars 1992, p. 114.

102.L'utilisation d'un micro-ordinateur ne constitue pas, en elle-même, un traitement automatisé dès lors qu'elle ne diffère pas de celle d'une machine à écrire, les données n'étant pas mémorisées à des fins de traitement ultérieur.

103.En revanche, la diffusion sur internet de données relatives à des chercheurs constitue un traitement automatisé au sens de la loi[45]. Par conséquent, l'utilisation de l'internet pour des activités de dialogue (« chat ») impliquant le traitement de données personnelles des participants ou d'autres personnes est également soumise aux règles de la loi Informatique et libertés modifiée sans qu'il s'agisse là d'une limitation à l'utilisation d'internet.

104.Dès lors qu'elles permettent la réalisation du traitement automatisé de données personnelles (collecte, enregistrement, consultation, transfert), les techniques de communication électronique entrent dans le champ d'application de la loi. Il en est ainsi de l'obligation de déclarer à la Cnil la mise en place d'un autocommutateur téléphonique[46].

105.Les systèmes permettant le contrôle d'accès par badge ou encore simplement l'identification des personnes pour l'accès logique à un système informatique doivent eux aussi être déclarés.

106.Il convient de noter que les traitements de données mis en œuvre pour l'exercice d'activité exclusivement personnel, lorsque leur responsable remplit les conditions prévues à l'article 5 de la loi Informatique et libertés modifiée, ne relève pas du champ d'application de la loi[47]. Il en est ainsi des agendas et autres carnets d'adresses personnels, dès lors qu'ils ne sont pas informatisés et qu'ils sont utilisés en dehors du cadre professionnel.

107.De même, les dispositions de la loi Informatique et Libertés ne sont pas applicables aux copies temporaires qui sont faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique, en vue du stockage automatique, intermédiaire et transitoire des données et à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises[48].

108.Sont, en revanche, soumis à la loi Informatique et libertés les traitements dont le responsable :

- est établi sur le territoire français ; le responsable d'un traitement qui exerce une activité sur le territoire français dans le cadre d'une installation, quelle que soit sa forme juridique, y est considéré comme établi ;

- sans être établi sur le territoire français ou sur celui d'un autre Etat membre de la Communauté européenne, recourt à des moyens de traitement situés sur le territoire français, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur ce territoire ou sur celui d'un autre Etat membre de la Communauté européenne[49].

-

109.La proposition de règlement du 25 janvier 2012 élargit le périmètre géographique de responsabilité prévoyant l'application du règlement :

- En cas de traitement des données effectué dans le cadre des activités d'un établissement d'un responsable de traitement ou d'un sous- traitant sur le territoire de l'Union Européenne.

[45] Cnil, Délib. n° 95-131 et n° 95-132 du 7-11-1995, 16ème rapport d'activité de la Cnil, p. 85.
[46] Cnil, Délib. n° 84-31 du 18-9-1984, 5ème rapport d'activité de la Cnil, p. 242 et Cnil, Délib. n° 94-113 du 20-12-1994, 15ème rapport d'activité de la Cnil, p. 79.
[47] Art. 2, al. 1 de la loi Informatique et libertés modifiée.
[48] Art. 4 de la loi Informatique et libertés modifiée.
[49] Art. 5 de la loi Informatique et libertés modifiée.

- En cas de traitement des données appartenant à des personnes concernées ayant leur résidence sur le territoire de l'Union Européenne, par un responsable qui n'est pas établi dans l'Union Européenne, lorsque les activités de traitement sont liées à des offres de bien et de services à ces personnes concernées dans l'Union Européenne ou à l'observation de leur comportement.
- En cas de traitement des données par un responsable du traitement qui n'est pas établi dans l'Union Européenne mais dans un lieu où la législation nationale d'un Etat membre s'applique en vertu du droit international public.

3.2.2 Les traitements non automatisés

110.La loi Informatique et libertés modifiée s'applique au traitement non automatisé de données personnelles contenues ou appelées à figurer dans des fichiers[50].

111.La loi précise la notion de « fichier de données personnelles », lequel est constitué par « tout ensemble structuré et stable de données à caractère personnel accessible selon des critères déterminés »[51].

112.Cette définition fait prévaloir le critère d'organisation du fichier.

113.Par sa part, la directive européenne 95/46/CE précise que le « fichier de données à caractère personnel » est constitué par « tout ensemble structuré, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique[52] ».

114.Un simple cahier dans lequel étaient conservées des informations sensibles collectées par un employeur à l'occasion de l'embauche de candidat a été assimilé à un fichier manuel[53].

115.Dans un arrêt très controversé, la Cour de cassation a adopté une interprétation restrictive de la notion de fichier, en estimant qu'un ensemble de dossier papier ne constituait pas un fichier, soumis en tant que tel à un régime juridique spécifique[54]. La majorité de la doctrine a fortement critiqué cette décision qui ne donne aucun critère de distinction entre la notion de fichier et celle de dossier.

116.Pour sa part, la Cnil ne considère pas cette décision comme un arrêt de principe, dans la mesure où elle permet selon elle de contourner l'esprit de la loi Informatique et libertés[55].

117.Le danger étant de voir se développer la création de traitement de données personnelle sur des supports ne relevant pas du champ d'application de la loi Informatique et libertés, les dispositions de cette même loi relative à la collecte, à l'enregistrement, à la conservation des données et aux droits d'accès ou d'opposition sont applicables aux fichiers non automatisés.

118.De même, les dispositions relatives aux formalités de déclaration préalable auprès de la Cnil s'appliquent.

[50] Art. 2, al. 1 de la loi Informatique et libertés modifiée.
[51] Art. 2, al. 4 de la loi Informatique et libertés modifiée.
[52] Art. 2-c de la directive 95/46/CE.
[53] TGI Créteil, 12ème ch. 10-7-1987 : D. 1988, p. 319, note J. Frayssinet.
[54] Cass. crim., 3-11-1987, Procureur Général c/ M. R. : expertise 1987 n° 101 p. 473.
[55] 8ème rapport d'activité de la Cnil, p. 220.

4. Les obligations du responsable du traitement

La loi informatique et liberté prône des principes fondamentaux que sont le principe de légalité, le principe de finalité, le principe de légitimité et le principe de confidentialité qui représentent autant d'obligations pour le responsable du traitement.

4.1 La licéité / le principe de légalité du traitement

119.La loi Informatique et libertés modifiée pose, en principe, qu'il est nécessaire de recueillir le consentement de la personne concernée afin de procéder à un traitement[56].

120.Toutefois, le responsable du traitement peut procéder au traitement en l'absence du consentement de la personne lorsque le traitement satisfait à l'une des conditions suivantes :

- le respect d'une obligation légale incombant au responsable du traitement ;
- la sauvegarde de la vie de la personne concernée ;
- l'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;
- l'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ;
- la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

121.La loi Informatique et libertés modifiée prévoit également que « les données sont collectées et traitées de manière loyale et licite[57] ».

122.La collecte illicite de données personnelles est sanctionnée par l'article 226-18 du Code pénal, lequel prévoit une amende de 300.000 euros et une peine d'emprisonnement de cinq ans. Pour les personnes morales, l'amende encourue est quintuplée, soit 1.500.000 euros, et s'accompagne des peines prévues à l'article 131-38 du Code pénal.

123.La Cnil considère comme déloyale et donc illicite :

- la collecte indirecte, c'est-à-dire auprès de tiers, opérée par la gendarmerie à l'insu des intéressés[58] ;
- l'obtention de numéros d'abonnés par sélection aléatoire ou par fabrication de séquences à partir d'un indicatif.

124.Dans ce domaine, la Cnil estime que si un automate d'appels compose aléatoirement des numéros de téléphone, la collecte est déloyale ou frauduleuse. Elle demande notamment au

[56] Art. 7 de la loi Informatique et libertés modifiée.
[57] Art. 6, 1° de la loi Informatique et libertés modifiée.
[58] Cnil, Délib. n°81-120 du 15-12-1981, 3ème rapport d'activité de la Cnil, p. 265.

responsable de l'automate d'appels d'obtenir le consentement préalable et express des abonnés qui vont être démarchés ce qui suppose une première démarche écrite auprès des prospects[59].

4.2 La détermination des finalités et les conséquences sur la qualité des données personnelles / le principe de finalité

125.La détermination de la finalité du traitement permet de préciser les limites dans lesquelles agit la personne qui procède au traitement. Ces finalités doivent être adaptées au but recherché et ne pas être étendues à d'autres fins.

126.Ainsi, la loi prévoit que les données personnelles soient collectées de manière loyale et licite.

127.A titre d'exemple, a été jugée déloyale, la compilation d'annonces immobilières de particuliers sur internet pour les revendre à des professionnels, cette collecte se faisant à l'insu des personnes[60].

128.Par ailleurs, les données personnelles « sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités[61] ».

129.Toutefois, un traitement ultérieur de données à des fins statistiques ou à des fins de recherches scientifiques ou historiques est considéré comme compatible avec les finalités initiales de la collecte des données s'il est réalisé dans les conditions fixées par l'article 6.

130.En outre, les données doivent être « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leur traitement ultérieur[62] ».

131.A titre d'exemple, la Cnil a adressé un avertissement à une société en raison de la création d'une liste des personnes ayant résilié leur autorisation de prélèvement automatique, dénommée « clients en résiliation définitive PA », contenant les données des clients ayant résilié ce mode de paiement[63].

132.Elles doivent être « exactes, complètes et, si nécessaire, mises à jour[64] ». Les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont déclarées ou traitées soient effacées ou rectifiées.

133.Enfin, les données peuvent être conservées « sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées[65] ».

[59] Cnil, Délib. n°84-31 du 18-9-1984, 5ème rapport d'activité de la Cnil, Cnil, Délib. n°85-79 du 10-12-1985, 6ème rapport d'activité de la Cnil, page 294 et Cnil, Délib. n°90-121 du 4-12-1990, 11ème rapport d'activité de la Cnil, p. 279.
[60] Cnil, Délib. n° 09-148 du 26-2-2009.
[61] Art. 6, 2° de la loi Informatique et libertés modifiée.
[62] Art. 6, 3° de la loi Informatique et libertés modifiée.
[63] Cnil, Délib. n°09-002 du 20-1-2009.
[64] Art. 6, 4° de la loi Informatique et libertés modifiée.
[65] Art. 6, 5° de la loi Informatique et libertés modifiée.

4.3 La sécurité et la confidentialité

4.3.1 Le contenu de l'obligation de sécurité et de confidentialité

134.La loi met à la charge du responsable du traitement une obligation de sécurité des données, ce dernier étant tenu « de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès[66] ».

135.Cette obligation s'applique à la fois aux traitements automatisés ou non automatisés.

136.Lorsque les données font l'objet d'une opération de traitement de la part d'un sous-traitant, ce dernier doit présenter des garanties suffisantes pour assurer la mise en œuvre de l'obligation de sécurité[67]. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures.

137.La Cour de cassation a estimé que les responsables de l'informatisation d'un syndicat interprofessionnel de médecins du travail n'ont pas respecté leurs obligations de sécurité dans la mesure où ils se sont bornés à diffuser plusieurs notes de service pour rappeler une évidence, à savoir qu'un mot de passe, doit rester personnel. Ils leur appartenaient, indépendamment des notes de service, de faire assurer la formation suffisante pour que chacun connaisse parfaitement le fonctionnement du système lequel, dès lors que les règles étaient respectées, ne permettait pas une telle intercommunication[68].

138.La violation de l'obligation de sécurité est assortie de sanctions pénales :

- cinq ans d'emprisonnement et 300.000 euros d'amende[69] pour les personnes physiques ;

- soit 1.500.000 euros, assortis des peines prévues à l'article 131-39 du Code pénal pour les personnes morales.

139.L'ordonnance du 24 août 2011 a inséré un article 34 bis à la loi informatique et libertés qui oblige les fournisseurs de services de communications électroniques accessibles au public à avertir sans délai la Cnil en cas de violations de données à caractère personnel.

140. Un règlement de la Commission européenne du 24 juin 2013[70] est venu compléter cette obligation de notification à la charge des fournisseurs de services de communication électronique accessible au public. Lorsque la violation de données à caractère personnel est susceptible de porter atteinte aux données à caractère personne ou à la vie privée d'un abonné ou d'un particulier, le fournisseur, en plus de prévenir la CNIL, doit notifier également la violation à l'abonné ou au particulier concerné.

[66] Art. 34 de la loi Informatique et libertés modifiée.
[67] Art. 35, al. 3 de la loi Informatique et libertés modifiée.
[68] Cass. crim., 30-10-2001 : Gaz. Pal. n°296-297 des 23 et 24-10-2002, som. P. 40, note Ariane Mole et Hélène Lebon.
[69] Art. 226-17 du C. pén.
[70] Règlement n° 611/2013 de la Commission du 24-06-2013 concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la directive 2002/58/CE du Parlement Européen et du Conseil sur la vie privée et les communications électroniques.

141.Cependant, cette notification n'est pas nécessaire dans le cas où la Cnil a constaté que des mesures de protection appropriées ont été mises en œuvre par le fournisseur pour rendre les données concernées incompréhensibles.

142.Le fournisseur de services de communications électroniques qui ne procède pas à la notification de la violation à la Cnil ou à l'intéressé encourt 5 ans d'emprisonnement et 300.000 euros d'amende.

4.3.2 Les préconisations de la Cnil

143.Si la loi n'impose aucune mesure technique précise pour mettre en œuvre l'obligation de sécurité, la Cnil a développé une « doctrine » importante sur ce point.

> 1°) La Commission a adopté en 1981 une recommandation relative aux mesures générales de sécurité des systèmes informatiques[71]. Cette recommandation à caractère général, rappelle qu'il appartient au détenteur ou utilisateur de traitement de prendre, sous sa responsabilité, les mesures nécessaires concernant notamment « le contrôle de la fiabilité des matériels et des logiciels », ainsi que « la capacité de résistance aux atteintes accidentelles ou volontaires extérieures ou intérieures ».

144.La Cnil recommande en particulier :

- l'évaluation des risques et études générales de la sécurité ;
- un effort d'information et de sensibilisation auprès des catégories professionnelles concernées ;
- la définition des dispositions destinées à assurer la sécurité et la confidentialité des traitements et des informations, ainsi que leur consignation dans un document de référence ;
- que les responsabilités des personnels participant au respect des mesures de sécurité soient clairement identifiées.

> 2°) Depuis cette recommandation à caractère général, la Cnil a précisé sa « doctrine », notamment en ce qui concerne les modalités d'attribution d'un mot de passe ou la composition de celui-ci. En particulier, elle préconise :

- l'attribution à chaque utilisateur d'un mot de passe personnel, quelle estime devoir être d'une longueur minimale de huit caractères ; dans la plupart des cas, la Cnil ajoute que ces six caractères doivent être composés de manière alphanumérique ;
- l'accès sélectif des utilisateurs aux informations ;
- la tenue d'un livre de bord de la sécurité, ou code de sécurité, consignant les dispositions prises pour assurer la sécurité et la confidentialité des traitements.

145.Dans sa recommandation du 1er juillet 2003 relative à la sécurité des systèmes de vote électronique sur place ou à distance, en particulier par internet, la Cnil émet un certain nombre de

[71] Cnil, Délib. n°81-94 du 21-7-1981 portant adoption d'une recommandation relative aux mesures de sécurité des systèmes informatiques, JO des 24 et 25-8-1981.

préconisations destinées à assurer l'anonymat et la confidentialité du vote ainsi que la transparence des systèmes informatique mis en œuvre[72].

146.La Cnil ne manque pas de vérifier à la fois dans les déclarations, demandes d'autorisation, les demandes d'avis qu'elle reçoit et à l'occasion des contrôle sur place, que le niveau de sécurité mis en œuvre est satisfaisant au regard de la nature des données traitées.

147.Ainsi, la Cnil a adressé un avertissement public à la société Free SAS pour avoir manqué à son obligation de sécurité en transmettant par erreur aux éditeurs d'annuaires et aux services de renseignements téléphoniques, le fichier des abonnés inscrit sur la « liste rouge ». La Cnil a considéré qu'il s'agissait d'un manquement aux dispositions de l'article 34 de la loi du 6 janvier 1978 modifiée en août 2004[73].

148.Dans le cadre des Assises de la sécurité, la Cnil a publié, en octobre 2010[74], un nouveau guide destiné à faciliter l'application par les responsables de traitements des prescriptions de la loi Informatique et libertés en matière de sécurité des données personnelles.

149.Il est associé à ce guide, constitué de 17 fiches thématiques, un questionnaire, disponible sur le site de la commission, qui permettra aux personnes intéressées d'apprécier le niveau de sécurité des traitements de données mis en œuvre par l'organisme auquel ils sont rattachés.

4.3.3 La jurisprudence

150.L'obligation de sécurité des données personnelles ne vise pas seulement les mesures physiques et logiques de protection du système informatique. Elle vise aussi la préservation de la fiabilité de la qualité des données enregistrées.

151.Ainsi, par décision du 15 février 1994, la Cour d'appel de Paris a condamné le président du GIE CPII pour atteinte à la sécurité de l'information, sur le fondement d'un manquement pour négligence de sécurité résultant de la loi Informatique et libertés, dans la mesure où il n'avait pas pris la précaution d'ajouter dans son fichier certaines données pour éviter le risque de confusion homonymique ; une personne avait donc été fichée à tort comme mauvais payeur[75].

4.3.4 L'obligation de déclarer à la Cnil les dispositifs de sécurité mis en oeuvre

152.Toute formalité préalable effectuée après de la Cnil relative à un traitement de données personnelles doit préciser si des règles permettant de contrôler l'accès à l'application sont mises en place et si des dispositions pour protéger le réseau des instructions extérieures sont prises.

153.Le déclarant doit également indiquer si les données personnelles elles-mêmes font l'objet d'une protection particulière (anonymisation, chiffrement, …).

154.Il convient de souligner que les dispositifs de sécurité mis en place constituent eux-mêmes souvent des traitements automatisés de données personnelles, dont la mise en œuvre peut être considérée comme illégale si elle n'a pas fait l'objet, elle-même, des formalités préalables.

---

[72] Cnil, Délib. n°03-036 du 1-7-2003 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique.
[73] Délib. n°2006-208 du 21-9-2006.
[74] Ce guide est accessible à l'adresse :
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_securite%20VD.pdf
[75] CA Paris, 11ème ch. 15-2-1994, Inédit, n°93/03512, confirmé par Cass. crim., 19-12-1995, Gaz. Pal. 1996, som. P. 418, note Ariane Mole.

155.En conséquence, les contrôles d'accès par badge, ou encore simplement l'identification des personnes pour l'accès logique à un système informatique entrent dans le champ d'application de la loi.

156.Il en est de même de la journalisation des accès à l'insu des personnes qui, si elle n'est pas déclarée, peut entraîner la mise en œuvre des sanctions pénales.

4.4 Vers un renversement de la charge de la preuve

157.En droit civil, le principe est que la charge de la preuve incombe au demandeur.

158. Or la proposition de règlement prévoit à l'article 22 que :

- « Le responsable du traitement adopte des règles internes et met en œuvre les mesures appropriées pour garantir, et être à même de démontrer, que le traitement des données à caractère personnel est effectué dans le respect du présent règlement ».
-

159.Il est alors légitime de se demander si l'article 22 n'énonce pas le principe d'un renversement de la charge de la preuve au détriment du responsable des données personnelles.

4.5 La transmission des données personnelles hors union européenne

160.La loi Informatique et libertés modifiée encadre strictement les transmissions de données personnelles entre le territoire français et un Etat n'appartenant pas à l'union européenne. Il s'agit là d'une disposition essentielle destinée à éviter le contournement des règles européennes par exportation de données personnelles vers un pays tiers non pourvu de règles protectrices.

161.La loi ne précise pas quelle peut être la forme du transfert. Selon les cas, celui-ci peut être destiné à un responsable du traitement ou à un sous-traitant.

162.Pour sa part, la Cnil considère qu'il y a transfert, quelle que soit la forme, y compris manuelle, dès lors que le responsable du traitement recours, à un moment ou à un autre, à des procédés automatisés de traitement de données personnelles[76]. Tel est le cas notamment de transferts de données personnelles par voie télématique, mais aussi de la circulation de support magnétique (disquette, bande, etc…) ou de support papier.

> 1°) En principe, les données personnelles ne peuvent être transférées vers un pays extérieur à l'Union européenne que « si cet Etat assure un niveau de protection suffisant de la vie privée et des libertés et des droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet »[77].

163.Le niveau de protection suffisant s'apprécie notamment en fonction des dispositions en vigueur dans l'Etat tiers, ainsi qu'au regard des mesures de sécurité qui y sont appliquées, des caractéristiques propres du traitement, telles que ses fins et sa durée, ainsi que de la nature, de l'origine et de la destination des données traitées[78].

[76] Premier rapport d'activité de la Cnil, p. 30.
[77] Art. 68, al. 1 de la loi Informatique et libertés modifiée.
[78] Art. 68, al. 2 de la loi Informatique et libertés modifiée.

2°) Toutefois, le principe de niveau de protection suffisant connaît des dérogations. Le responsable du traitement peut transférer des données personnelles vers un pays tiers ne disposant pas d'un tel niveau si la personne concernée a consenti expressément au transfert des données personnelles ou si le transfert est nécessaire :

- à la sauvegarde de la vie de cette personne ;
- à la sauvegarde de l'intérêt public ;
- au respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice ;
- à la consultation d'un registre public dans les conditions prévues par la loi ;
- à l'exécution d'un contrat entre le responsable du traitement et l'intéressé, ou de mesures précontractuelles prises à la demande de celui-ci ;
- à la conclusion ou l'exécution d'un contrat conclu ou à conclure dans l'intérêt de la personne concernée, entre le responsable du traitement ou un tiers[79].

164.De la sorte, des données personnelles peuvent être transférées hors Union européenne vers un pays tiers n'assurant pas un niveau de protection suffisant par décision de la Cnil ou par décret en Conseil d'Etat pour certains traitements relevant de la sphère publique.

165.De plus, le transfert de données personnelles vers un pays tiers n'assurant pas un niveau de protection suffisant peut avoir lieu lorsque le traitement garantit un niveau de protection suffisant notamment en raison des clauses contractuelles ou règles internes dont il fait l'objet[80].

166.Ces dispositions relatives aux flux transfrontières ne s'appliquent pas aux données personnelles traitées aux fins de journalisme et d'expression littéraire ou artistique.

167.Les transferts de données personnelles envisagés vers un pays tiers à l'Union doivent faire l'objet de formalités préalables auprès de la Cnil. En effet, ces traitements ne peuvent pas bénéficier des allègements de formalités déclaratives. La Cnil peut requérir un certain nombre de garanties lors de la déclaration, demande d'autorisation ou demande d'avis, si elle considère que l'Etat destinataire des données personnelles transférées ne dispose pas d'une protection suffisante au regard de la loi française Informatique et libertés modifiée.

3°) La directive européenne 95/46/Ce interdit tout transfert vers un pays tiers à la Communauté européenne si ce pays n'assure pas un niveau dit de « protection adéquat » au regard de la vie privée et des libertés et droits fondamentaux des personnes. C'est la Commission européenne qui détermine si un pays tiers dispose d'une protection adéquate[81].

168.D'ores et déjà, plusieurs pays tiers ont été reconnus comme disposant d'un niveau de protection adéquat permettant le libre transfert de données personnelles depuis la Communauté. Il s'agit de la Suisse, du Canada, de Guernesey, l'Isle de Man, de l'Argentine, de Jersey, des iles Féroé

[79] Art. 69 de la loi Informatique et libertés modifiée.
[80] Art. 69 de la loi Informatique et libertés modifiée.
[81] Voir http://europa.eu.int/comm/internal_market/privacy/adequacy-fr.htm

et d'Andorre, l'Etat d'Israël. Récemment, la Nouvelle-Zélande a été reconnue comme bénéficiant d'une protection adéquate le 19 décembre 2012 par la Commission européenne[82].

169.De plus, la Commission européenne a élaboré des clauses contractuelles types offrant des garanties adéquates. Ces clauses mettent à la charge de l'exportateur et de l'importateur des données personnelles un certain nombre d'obligations. Ainsi, l'importateur s'engage à ne traiter les données transférées que pour le compte exclusif de l'exportateur et conformément à ses instructions[83].

170.Par ailleurs, les entreprises peuvent mettre en place des Règles Internes d'Entreprise (Binding Corporate Rules). Ces BCR constituent un code de conduite concernant la politique interne du groupe en matière de transfert de données à caractère personnelles hors de l'Union Européenne. Elles permettent le transfert, au sein d'une entreprise ou d'un groupe, de données à caractère personnel depuis l'Union européenne vers des pays tiers à l'Union sans qu'une autorisation préalable ne soit nécessaire.

171.Enfin, la Communauté européenne et les Etats-Unis ont conclu un accord dénommé « Safe Harbor »[84] (ou sphère de sécurité). Cet accord permet aux entreprises américaines de souscrire volontairement à une série de principes afin de pouvoir être considérées comme assurant, en interne, un niveau de protection adéquat leur permettant de traiter des données personnelles en provenance de la Communauté européenne.

> 4°) Avant l'adoption de la directive européenne 95/46/CE, la Cnil avait examiné le transfert de données personnelles de la France vers l'Italie relative à la gestion du personnel de la société Fiat.

172.Observant que l'Italie ne disposait pas d'une législation de protection des données personnelles à cette époque, la Cnil a subordonné la transmission des données personnelles à la signature par Fiat Italie d'un contrat, par lequel cette société s'engageait à respecter l'ensemble des dispositions de la loi française et de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[85].

5. Les droits de la personne concernée

173.La protection de la vie privée et plus particulièrement la protection des données personnelles sont respectées à travers le respect de certains droits parmi lesquels on trouve principalement :

- Le droit à l'information
- Le droit de rectification et d'interrogation

[82] Décis. N°2013/65/UE de la Commission du 19-12-2012 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la Nouvelle-Zélande.

[83] Décis. n°2001/497/CE de la Commission du 15-6-2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu de la directive 95/46/CE,JOCE du 4-7-2001, p. 19 ; décision 2002/16/CE de la Commission du 27-12-2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE, JOCE L du 10-1-2002, p. 52 ; décision 204/915/CE de la Commission du 27-12-2004 modifiant la décision 2001/497/CE en ce qui concerne l'introduction d'un ensemble alternatif de clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers, JOCE L du 29-12-2004, p. 74.

[84] Décis. 2000/520/CE de la Commission européenne du 26-7-2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiées par le ministère du commerce des Etats-Unis d'Amérique, JOCE L du 25-8-2000, p.7.

[85] Cnil, Délib. n°89-78 du 11-7-1989, 10ème rapport d'activité de la Cnil, p. 32.

- Le droit d'opposition
- Le droit de ne pas être soumis à une décision prise à partir de profils
- L'émergence d'un droit à l'oubli.

5.1 Le droit d'information

174.La loi prévoit à la charge du responsable du traitement une obligation générale d'information de la personne concernée quel que soit le mode de collecte des données personnelles.

175.Cette obligation a pour but de permettre à la personne concernée de contrôler l'utilisation des données personnelles pour ensuite exercer les droits individuels que la loi lui confère : droit d'accès et de rectification, droit d'opposition, droit de ne pas voir effectué le traitement de données sensibles et, enfin, droit de ne pas être soumise à une décision prise à partir de profil.

5.1.1 Le droit d'information lors d'une collecte directe de données personnelles

176.Lorsque les données personnelles sont recueillies directement auprès de la personne concernée, le responsable du traitement ou son représentant doivent lui fournir un certain nombre d'informations[86]. Ces informations portent sur les éléments suivants :

- l'identité du responsable du traitement et, le cas échéant, celle de son représentant ;
- la finalité poursuivie par le traitement auquel les données sont destinées ;
- le caractère obligatoire ou facultatif des réponses ;
- les conséquences éventuelles, à son égard, d'un défaut de réponse ;
- les destinataires ou catégorie de destinataires des données ;
- les droits d'opposition ;
- le droit d'interrogation.
- le cas échéant, l'existence de transfert de données personnelles envisagé à destination d'un Etat non-membre de la Communauté européenne.

177.L'information peut, en principe, être effectuée par tout moyen, sauf lorsque les données sont collectées sous forme de questionnaire.

178.Cette obligation large d'information s'applique notamment à tous les procédés de contrôle d'accès, aux systèmes d'horaires variables, aux autocommutateurs téléphoniques mis en place sur le lieu de travail et aux automates d'appels. A cet égard, la Cnil impose une information préalable des salariés sur les caractéristiques des traitements mis en place.

179.Lorsqu'il est procédé à la collecte d'informations via internet, la Commission considère que les mentions d'information doivent apparaître à l'écran.

180.Lorsque la collecte des données se fait par voie de questionnaire, seules certaines de ces informations doivent être fournies à la personne concernée.

[86] Article 32-1 de la loi informatique et liberté modifiée

181.Le responsable du traitement ou son représentant ne sont pas tenus de fournir ces informations lorsque la personne a été informée au préalable.

182.Un décret[87] institue des contraventions de police à l'égard de tout responsable du traitement qui ne se serait pas conformé à son obligation d'information.

5.1.2 L'information de la personne utilisatrice des réseaux de communication électronique

183.Lorsque la collecte des données se fait par voie des réseaux de communication électronique, la loi prévoit l'obligation d'informer « de manière claire et complète » la personne concernée[88]. L'information, apportée de manière claire et complète, doit porter sur les éléments suivants :

- la finalité de toute action tentant à accéder, par voie de transmission électronique, à des informations stockées dans son équipement terminal de connexion, ou à inscrire, par la même voie, des informations dans son équipement terminal de connexion ;

- les moyens dont elle dispose pour s'y opposer.

184.Cet article a été modifié par l'ordonnance n°2011-1012 du 24 août 2011 relative aux communications électroniques. Il a été ajouté l'obligation pour le responsable de traitement d'avoir recueilli l'accord, de l'utilisateur ou de l'abonné informé, à ces accès ou inscriptions. Il est précisé que cet accord « peut résulter de paramètres appropriés de son dispositif de connexion ou de tout autre dispositif placé sous son contrôle ».

185.Cependant, le responsable du traitement n'a pas à fournir ces informations si l'accès aux informations stockées ou l'inscription de la formation dans l'équipement terminal de l'utilisateur :

- soit a pour finalité exclusive de permettre ou faciliter la communication par voie électronique ;

- soit est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur.

5.1.3 L'obligation d'information lors d'une collecte indirecte de données personnelles

186.Lorsque les données personnelles ne sont pas recueillies auprès de la personne concernée, le responsable du traitement ou son représentant doit fournir à cette dernière les mêmes informations que celles qu'il est tenu de délivrer en cas de collecte directe.

187.Cette information doit être donnée dès l'enregistrement des données ou, si une communication des données à des tiers est envisagée, au plus tard lors de la première communication des données[89].

188.L'obligation d'information connaît néanmoins cinq exceptions lorsque :

- les données ont été recueillies initialement pour un autre objet mais que le traitement est effectué à des fins historiques, statistiques ou scientifiques ;

[87] Décr. 81-1142 du 23-12-1981.
[88] Art. 32, II de la loi Informatique et libertés modifiée.
[89] Art. 32-III de la loi Informatique et libertés modifiée.

- la personne concernée est déjà informée ;

- l'information de la personne concernée se révèle impossible ou exige des efforts disproportionnés par rapport à l'intérêt de la démarche ;

- les données recueillies sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation ;

- le traitement a pour objet la prévention, la recherche, la constatation ou la poursuite d'infractions pénales[90].

189.En outre, le responsable du traitement doit fournir des informations spécifiques à la personne concernée lorsque les données recueillies sont utilisées à des fins de recherche dans le domaine de la santé.

5.2 Le droit d'interrogation et de rectification

5.2.1 Le droit d'interrogation

190.Véritable droit de regard, le droit d'interrogation permet d'éviter les dérives et d'encourager la transparence du traitement de données personnelles, quel que soit le secteur privé ou public et le mode de traitement[91].

191.Le droit d'interrogation permet, dans un premier temps, à la personne, de questionner le responsable du traitement afin de savoir si ce traitement contient ou non les données la concernant.

192.Il offre ensuite la possibilité au demandeur de connaître le détail des données le concernant, et s'il le souhaite, la logique qui sous-tend le traitement.

193.Bien que la loi ne le précise pas expressément, le droit d'interrogation semble appartenir aux seules personnes physiques. Un arrêt du Conseil d'Etat a, en effet, reconnu la légalité du refus d'accès à une personne morale, en l'occurrence l'église de scientologie[92].

194.Toutefois, par délibération du 3 juillet 1984, la Cnil a émis un avis plus nuancé, en précisant que si le droit d'accès a un caractère strictement individuel, il convient d'en reconnaître l'exercice aux personnes physiques, représentants légaux des entreprises, dès lors que le nom de ces personnes figure dans le fichier en tant que dirigeant, actionnaire ou associé[93].

195.Par ailleurs, la personne qui entend exercer son droit d'interrogation n'a aucune justification à donner.

196.A cet égard, à condition de justifier de son identité, la personne a le droit d'obtenir :

- la confirmation que des données personnelles la concernant font ou ne font pas l'objet de ce traitement ;

[90] Art. 32-III, IV et VI de la loi Informatique et libertés modifiée.
[91] Art. 39 de la loi Informatique libertés modifiée.
[92] CE, 15-2-1991, Eglise de scientologie c/Conseil d'Etat, Expertises 1991, p. 322.
[93] Cnil, Délib. n°84-28 du 3-7-1984, commentaire J. Frayssinet, Dalloz 1984, p. 587.

- des informations relatives aux finalités du traitement, aux catégories de données personnelles traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées ;

- des informations relatives au transfert de données envisagé à destination d'un Etat non-membre de la Communauté européenne ;

- la communication, sous une forme accessible, des données la concernant ainsi que de toute information disponible quant à l'origine de ces données ;

- des informations permettant de connaître et de contester le régime qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à son égard.

197.Toutefois, les informations communiquées ne doivent pas porter atteinte aux droits d'auteur au sens des dispositions du livre premier et du titre IV du livre III du Code de la propriété intellectuelle.

198.Le droit d'interrogation ne s'applique pas lorsque les données sont conservées sous une forme excluant manifestement tout risque d'atteinte à la vie privée de la personne concernée et pendant une durée n'excédant pas celle nécessaire aux seules finalités d'établissement de statistiques ou de recherches scientifiques ou historiques.

199.L'exercice du droit d'interrogation n'est assorti d'aucune condition de périodicité. Toutefois, le responsable du traitement peut s'opposer aux demandes manifestement abusives, notamment par leur nombre, leur caractère répétitif ou systématique[94]. En cas de contestation, c'est le responsable du traitement qui doit prouver le caractère manifestement abusif des demandes.

5.2.2 Le droit de rectification

200.Le droit de rectification est un droit complémentaire au droit d'interrogation. Il n'est cependant pas soumis aux mêmes conditions d'exercice.

201.Ainsi, toute personne physique peut exiger du responsable du traitement que soient rectifiées, complétées, mises à jour, verrouillées ou effacées les données la concernant, qui sont inexactes, incomplètes, équivoques, périmées ou dont la collecte, l'utilisation, la communication ou la conservation est interdite[95].

202.Lorsque la personne concernée obtient une modification de l'enregistrement, elle bénéficie du remboursement des frais correspondant au coût de la copie.

203.Ce complément naturel du droit d'accès est lui-même prolongé par l'obligation pour le responsable du traitement, si une donnée a été transmise à un tiers, d'accomplir « les diligences utiles afin de lui notifier les opérations qu'il a effectuées conformément à la demande de la personne concernée »[96].

204.En outre, la loi prévoit que les héritiers d'une personne décédée peuvent exiger du responsable du traitement de prendre en considération le décès de la personne et procéder en conséquence à des mises à jour[97].

[94] Art. 39, II de la loi Informatique et libertés modifiée.
[95] Art. 40 de la loi Informatique et libertés modifiée.
[96] Art. 40, al. 5 de la loi Informatique et libertés modifiée.
[97] Art. 40, al. 6 de la loi Informatique et libertés modifiée.

205.Lorsque la personne concernée exerce son droit de rectification, elle n'a pas besoin de justifier sa démarche ou de la motiver. Il suffit simplement qu'elle justifie de son identité et que les informations soient inexactes, incomplètes, équivoques, etc.

5.3 Le droit d'opposition

206.Toute personne physique a le droit de s'opposer, « pour des motifs légitimes », à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement[98].

207.La loi ne précise pas ce que peuvent être des « motifs légitimes » motivant un refus. Leur reconnaissance reste donc soumise, au cas par cas, à l'appréciation des tribunaux lesquels se réfèrent généralement aux dispositions du Code civil relatives à la protection de la vie privée.

208. La proposition de règlement du 25 janvier 2012 a d'ailleurs remplacé la condition de « motifs légitimes » du droit d'opposition par la condition de « raisons tenant à la situation particulière de la personne concernée ».

209.La loi prévoit un second cas de droit d'opposition. Ce dernier s'exerce sans frais et sans raison légitime lorsque les personnes concernées souhaitent s'opposer à l'utilisation de leurs données à des fins de prospection, notamment commerciale[99].

210. La proposition de règlement du 25 janvier 2012 n'utilise là encore pas la même terminologie, prévoyant un droit d'opposition lors que les données des personnes concernées sont traitées à des « fins de marketing direct ».

211. La Cnil a fait usage de son pouvoir de sanction à l'encontre d'une société ayant procédé à des opérations de prospection commerciale par télécopie sans avoir obtenu, conformément à la loi, le consentement préalable des personnes physiques concernées, et surtout sans tenir compte des demandes d'opposition qui avaient été formulées par les destinataires de ces télécopies[100].

212.L'Union française du marketing direct (UFMD) a créé à cet effet, un fichier "Robinson", dit "stop publicité" permettant à toute personne qui ne désire pas être démarchée par courrier ou par téléphone, d'être radiée des fichiers des entreprises adhérentes.

213.France Télécom dispose également de différentes listes d'opposition. La liste "Orange", par exemple, permet de rassembler les personnes qui ne souhaitent pas que leurs coordonnées soient commercialisées mais qui désirent néanmoins continuer à figurer dans l'annuaire téléphonique.

214.Avant la modification de la loi Informatique et libertés, le Conseil d'Etat a confirmé une décision de la Cnil de donner un avertissement à une société qui avait retiré de ses questionnaires une case à cocher permettant aux personnes d'exprimer leur opposition et l'avait remplacée par une mention leur rappelant leur droit de s'opposer à la commercialisation de leurs données à des fins de prospection[101].

215.Par ailleurs, la loi pour la confiance dans l'économie numérique du 21 juin 2004 prévoit un dispositif dit d'« opt-in » en matière de prospection directe par voie électronique[102].

[98] Art. 38, al. 1, de la loi Informatique et libertés modifiée.
[99] Art. 38, al. 2, de la loi Informatique et libertés modifiée.
[100] Cnil, Délib 2010-232 du 17-6-2010.
[101] CE, 30-7-1997, 10ème et 7ème SSR : RJAD 1/98 n 119.
[102] Loi n°2004-575 du 21-6-2004 pour la confiance dans l'économie numérique.

216.Si le droit d'opposition s'exerce à toutes les données personnelles, qu'elles résultent ou non d'un traitement automatisé, il ne peut être exercé que par une personne physique à l'égard de données qui doivent la concerner personnellement.

217.La question du droit d'opposition des personnes morales se pose néanmoins si, dans un traitement concernant une entreprise, figurent des données qualifiant la personnalité même du dirigeant. Dans cette hypothèse, il s'agirait alors de données personnelles. Les dirigeants pourraient alors disposer d'un droit d'opposition, sous réserve de pouvoir faire valoir des raisons légitimes.

218.Le fait de procéder à un traitement de données malgré l'opposition de la personne est puni de cinq ans d'emprisonnement et de 300.000 euros d'amende[103].

219.Le droit d'opposition ne s'applique pas aux traitements répondant à une obligation légale ou lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte autorisant le traitement[104].

5.4 Le droit de ne pas effectuer de traitement de données « sensibles »

220.Afin de protéger la vie privée et les libertés des personnes concernées, la loi limite le traitement de certaines données considérées comme sensibles.

5.4.1 Les données visées par l'article 8-I de la loi Informatique et Libertés modifiée

221.Les « catégories particulières de données », dont la collecte et le traitement sont interdits, comprennent tout d'abord les données qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci[105].

222.Le traitement de telles données est interdit, sauf à relever de l'une des exceptions prévues par la loi[106]. Ces exceptions couvrent un large champ de dérogation dans la mesure où la finalité du traitement l'exige. En particulier, l'interdiction de traiter les données peut être levée avec le consentement exprès de la personne concernée.

5.4.2 Le numéro d'identification au Répertoire national d'identification des personnes physiques

223.La loi considère ensuite les renseignements contenus dans le numéro d'identification au Répertoire national d'identification des personnes physiques (RNIPP), le numéro qui équivaut au numéro de sécurité sociale, comme étant des données sensibles. C'est pourquoi leur utilisation est soumise à autorisation.

224.Ainsi, pour limiter l'usage abusif qui pourrait être fait de telles informations, toute utilisation du numéro d'inscription au « RNIPP » pour effectuer des traitements de données est soumise à

[103] Art. 226-18-1 du C. pén.
[104] Art. 38, al. 3, de la loi Informatique et libertés modifiée.
[105] Art. 8, I de la loi Informatique et libertés modifiée.
[106] Art. 8, II à IV de la loi Informatique et libertés modifiée.

autorisation de la Cnil[107]. En revanche, le traitement du numéro identifiant mis en œuvre pour le compte de l'Etat, d'une personne morale de droit privé gérant un service public peut être autorisé par décret du Conseil d'Etat après avis motivé et publié de la Cnil[108].

225.Le fait d'utiliser le numéro d'identification au RNIPP hors des cas prévus par la loi est puni de cinq d'emprisonnement et de 300.000 euros d'amende[109].

226.L'interdiction de ne pas traiter des données sensibles ne s'applique pas aux organismes de la presse écrite ou audiovisuelle afin de ne pas limiter l'exercice de la liberté d'expression[110]. Cette exonération ne s'applique que lorsque les organismes diffusent le contenu de leur publication sur le minitel et sur internet. Elle ne les décharge pas de leur responsabilité.

5.5 Le droit de ne pas être soumis à une décision prise à partir de profils

227.La loi n'interdit pas les opérations de tri et de sélection qui peuvent être effectuées à partir d'un traitement automatisé de données. Ces opérations permettent notamment une division de données en vue de distinguer celles qui seront utilisées et celles qui ne le seront pas. Il s'agit par exemple de la segmentation de la clientèle et du ciblage permettant d'établir des profils types de consommateurs.

228.Pour autant, la loi pose un principe général : aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données destinées à évaluer certains aspects de sa personnalité[111].

229.En outre, aucune autre décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité[112].

230.En revanche, la loi précise que ne sont pas regardées comme prises sur le seul fondement d'un traitement automatisé les décisions prises dans le cadre de la conclusion ou de l'exécution d'un contrat et pour lesquelles la personne concernée était mise à même de présenter ses observations, ni celles satisfaisant les demandes de la personne concernée[113].

231.Cela signifie que l'informatique peut fournir une aide à la décision, mais qu'en aucun cas elle ne peut être l'unique base de cette décision, l'appréciation humaine devant avoir sa place.

232.A l'occasion d'une délibération d'avril 1993, la Cnil a élaboré sa doctrine en matière de segmentation comportementale à l'attention des établissements bancaires. La Commission précise que les critères de classement doivent avoir une certaine pertinence et que les informations du profil deviennent des informations communicables aux intéressés dès lors qu'elles peuvent être rattachées à une personne physique identifiée[114].

[107] Art. 25 de la loi Informatique et libertés modifiée.
[108] Art. 27 de la loi Informatique et libertés modifiée.
[109] Art. 226-16-1 du C. pén.
[110] Art. 67 de la loi Informatique et libertés modifiée.
[111] Art. 10, al. 1 de la loi Informatique et libertés modifiée.
[112] Art. 10, al. 1 et al. 2, de la loi Informatique et libertés modifiée.
[113] Art. 10, al. 3 de la loi Informatique et libertés modifiée.
[114] Cnil, Délib. n° 93-032 du 6-4-1993 : 14ème rapport d'activités p. 60.

233.Cette délibération a fait l'objet d'un pourvoi en annulation pour excès de pouvoir. Le Conseil d'Etat a estimé le recours recevable mais non fondé, la Cnil ayant fait une application correcte de la loi[115].

5.6 Le droit à l'oubli

234.Le législateur a mis implicitement en œuvre un droit à l'oubli numérique.

L'article 6.5 de la loi Informatiques et Libertés prévoit en effet que :

- « Les données à caractère personnels sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées ».

235.La durée de conservation des informations est ainsi appréciée au regard de la finalité des traitements par le Cnil.

236.Elle est notamment déterminée de façon à ce qu'une information emportant un jugement parfois négatif sur une personne, ne puisse lui être opposée, sauf justification légale, toute sa vie.

237.La proposition de règlement du 25 janvier 2012 va plus loin, prévoyant un droit à l'oubli numérique et à l'effacement [116] :

« La personne concernée a le droit d'obtenir du responsable du traitement l'effacement de données à caractère personnel la concernant et la cessation de la diffusion de ces données, en particulier en ce qui concerne des données à caractère personnel que la personne concernée avait rendues disponibles lorsqu'elle était enfant, ou pour l'un des motifs suivants:
a) les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées,
b) la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a), ou lorsque le délai de conservation autorisé a expiré et qu'il n'existe pas d'autre motif légal au traitement des données;
c) la personne concernée s'oppose au traitement des données à caractère personnel en vertu de l'article 19;
d) le traitement des données n'est pas conforme au présent règlement pour d'autres motifs ».

6. Les formalités préalables à la mise en œuvre des traitements

238.La loi Informatique et libertés, dans son ancienne version, établissait deux régimes distincts : l'un pour le secteur public, l'autre pour le secteur privé. Ce choix, basé sur le statut de l'organe qui mettait en œuvre le traitement, se justifiait par le fait que les administrations étaient dans les années 80 les principaux organismes à menacer les droits et libertés des personnes.

239.Depuis, la menace s'est progressivement déplacée vers le secteur privé et l'on constate une interpénétration croissance du secteur public et du secteur privé.

240.Cette évolution explique la nécessité d'instaurer une protection prenant en compte essentiellement les risques présentés par les traitements.

[115] CE Section contentieux 10ème et 7ème SSR 7-6-1995 : AJDA 12/95 p. 1110.
[116] Proposition RÈGL. DU PARLEMENT EUROPÉEN ET DU CONSEIL 2012/2011 du 25 janvier 2012 Art. 17

6.1 Les différentes formalités préalables

241.La loi Informatique et libertés distingue désormais deux types de formalités préalables : les traitements soumis à la procédure générale de déclaration et ceux soumis à la procédure exceptionnelle d'autorisation.

242.Certains traitements ne sont cependant soumis à aucune formalité préalable. Il s'agit de ceux qui ont pour seul objet la tenue d'un registre destiné exclusivement à l'information du public et ouvert à la consultation de ce dernier en vertu de dispositions législatives ou réglementaires[117], et de ceux dont la finalité se limite à assurer la conservation à long terme de documents d'archives au titre de l'article L. 212-4 du code du patrimoine[118].

6.1.1 La déclaration

6.1.1.1La déclaration ordinaire

243.En principe, les traitements doivent faire l'objet d'une déclaration auprès de la Cnil[119].

244.Une telle procédure n'est pas soumise à un contrôle de fond de la part de la Commission puisqu'elle ne fait l'objet que d'un simple enregistrement.

245.L'examen de la déclaration ordinaire donne simplement lieu lorsque le dossier est complet, à la délivrance sans délai d'un récépissé qui permet au déclarant de mettre en œuvre le traitement.

246.Cependant, en pratique, la Cnil n'hésite pas à demander au déclarant des précisions complémentaires sur un dossier imprécis. Au besoin, la Commission ne manque pas de rappeler expressément au déclarant que l'accomplissement des formalités de déclaration ne l'exonère en aucun cas de ses responsabilités au regard de l'application de la loi.

247.Les traitements relevant d'un même organisme ou ayant des finalités identiques ou liées entre elles peuvent faire l'objet d'une déclaration unique.

6.1.1.2La déclaration simplifiée

248.Pour les catégories les plus courantes de traitement, la Cnil a la possibilité d'établir et de publier des normes destinées à simplifier l'obligation de déclaration[120].

249.A ce jour, la Commission a adopté plus de cinquante normes simplifiées. En particulier, la norme 47 concerne les traitements mis en œuvre dans le cadre de l'utilisation de la téléphonie fixe et mobile sur les lieux de travail.[121]

250.En pareil cas, le déclarant doit effectuer une déclaration simplifiée de conformité à la norme. Cette formalité constitue de sa part un engagement à respecter la totalité des prescriptions et des caractéristiques posées dans le texte de la norme simplifiée.

251.A défaut, ou dans le cas où il existerait un doute sur la conformité du traitement à l'une des normes établies, la Cnil, contrairement au principe qui veut que le récépissé soit délivré sans délai, peut surseoir à cette délivrance et envisager une délibération sur le traitement en question.

[117] Art. 27, II, 1° de la loi Informatique et libertés modifiée.
[118] Art. 36, al. 2 de la loi Informatique et libertés modifiée.
[119] Art. 22 de la loi Informatique et libertés modifiée.
[120] Art. 24, I de la loi Informatique et libertés modifiée.
[121] Délib. n° 2005-019 du 3-2-2005.

252.La Commission peut alors entendre toute personne dont l'audition pourrait être utile à l'espèce, le déclarant étant pour sa part invité à justifier la conformité du traitement qu'il projette avec la norme simplifiée, ou, à défaut, à se soumettre au droit commun, c'est-à-dire à procéder à une déclaration ordinaire ou à une demande d'autorisation.

6.1.1.3La dispense de déclaration

253.La Cnil peut définir les catégories de traitement dispensées de déclaration[122].

254.Cette dispense est définie et accordée par la Commission Nationale de l'Informatique et des Libertés à partir des catégories de traitements considérés comme les plus courants au regard de leur finalité, de leurs destinataires ou catégorie de destinataires, des données à caractère personnel traitées, de la durée de consommation de celles-ci et des catégories de personnes concernées.

255.Cette simplification du régime déclaratif constitue par ailleurs un enjeu juridique pour les responsables de traitement dès lors que l'article 226-16 du Code pénal dispose que le fait de ne pas respecter, y compris par négligence, les normes simplifiées ou d'exonération établies par la Cnil est punie de 5 ans d'emprisonnement et de 300.000 € d'amende.

256.A ce jour, la Commission a adopté plus de dix-huit délibérations décidant de la dispense de déclaration de traitements.

6.1.1.4La déclaration de modification

257.Le déclarant est tenu d'informer la Cnil de la modification ou de l'évolution de son traitement. Cette formalité suit la même procédure que la déclaration ordinaire. Le déclarant établit à partir du même formulaire, une déclaration de modification précisant les principales caractéristiques du traitement et les modifications subies.

258.La notion de modification est large. Ainsi, la reprise d'un traitement à la suite d'une fusion ou d'une absorption d'entreprise par une autre est assimilée à une modification comportant pour le repreneur l'obligation de la déclarer.

6.1.1.5La déclaration de suppression

259.Toute suppression définitive d'un traitement doit être portée à la connaissance de la Cnil par le biais d'une déclaration de suppression. Cette déclaration est très succincte puisqu'elle ne comprend que les indications permettant l'identification du traitement supprimé.

260.La déclaration de suppression concerne l'abandon d'un traitement automatisé de données personnelles mais, en aucun cas, le simple archivage des données ou des résultats des raisonnements programmés, ou encore à l'expiration du délai légal de conservation du traitement.

6.1.2 L'autorisation

261.Pour les traitements de données considérés comme dangereux pour les droits et libertés des personnes, la loi définit un régime complexe d'autorisation.

262.Huit catégories de traitement ne peuvent être mises en œuvre qu'après autorisation de la Cnil[123].

[122] Art. 24, II de la loi Informatique et libertés modifiée.
[123] Art. 25, I de la loi Informatique et libertés modifiée.

263.Ces traitements portent sur :

- certaines données sensibles ;
- les données génétiques ;
- les données relatives aux infractions, condamnations ou mesures de sûreté ;
- les traitements susceptibles d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat ;
- les traitements automatisés ayant pour objet l'interconnexion de fichiers relevant d'une ou de plusieurs personnes morales gérant un service public et dont les finalités correspondent à des intérêts publics différents,
- les traitements automatisés ayant pour objet l'interconnexion de fichiers relevant d'autres personnes et dont les finalités principales sont différentes ;
- les traitements portant sur le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques et ceux qui requièrent une consultation de ce répertoire ;
- les traitements comportant des appréciations sur les difficultés sociales des personnes ;
- les traitements comportant des données biométriques nécessaires au contrôle de l'identité des personnes.

264.Ces traitements considérés comme sensibles ne peuvent pas être mis en œuvre sans l'autorisation préalable de la CNIL et son soumis à une procédure d'examen renforcé par les services de la CNIL ;

265.La Cnil doit se prononcer dans un délai de deux mois à compter de la réception de la demande, ce délai pouvant être renouvelé une fois.

266.Lorsqu'elle ne se prononce pas dans ces délais, la demande d'autorisation est réputée rejetée.

267.Les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires peuvent être autorisés par une décision unique de la Cnil. Dans ce cas, le responsable de chaque traitement adresse à la Commission un engagement de conformité de celui-ci à la description figurant dans l'autorisation[124].

268.D'autres traitements sont autorisés par arrêté du ou des ministres compétents, pris après avis motivé et publié de la Cnil[125], d'autres encore par décret en Conseil d'Etat toujours pris après avis motivé de la Cnil[126].

269.Enfin, certains traitements sont autorisés par simple arrêté ou, en cas de traitement opéré pour le compte d'un établissement public ou d'une personne morale de droit privé et gérant un service

[124] Art. 25, II de la loi Informatique et libertés modifiée.
[125] Art. 26, I de la loi Informatique et libertés modifiée.
[126] Art. 26, II de la loi Informatique et libertés modifiée.

public, par décision de l'organe délibérant chargé de leur organisation, pris après avis motivé et publié de la Cnil[127].

270.Le non-respect des formalités préalables est sanctionné pénalement, le responsable du traitement encourant cinq ans d'emprisonnement et 300.000 euros d'amende[128]. Il en va de même pour le non-respect des normes simplifiées ou de la dispense d'exonération[129].

6.2 La nomination d'un correspondant à la protection des données à caractère personnel

271.La loi Informatique et Libertés modifiée prévoit une innovation majeure : sont dispensés des formalités préalables les traitements de données pour lesquels le responsable a désigné un correspondant à la protection des données à caractère personnel chargé d'assurer « de manière indépendante » l'application des obligations prévues par la loi[130].

272.Cette possibilité ne s'applique pas lorsqu'un transfert de données personnelles à destinations d'un Etat non-membre de la Communauté européenne est envisagé.

6.2.1 Intérêts

273.La désignation d'un correspondant à la protection des données, appelé également Correspondant Informatique et Libertés (CIL) par la Cnil, présente plusieurs intérêts pratiques.

274.Outre le fait de dispenser le responsable du traitement des formalités préalables, le recours au Cil permet de participer à la mise en œuvre d'une approche qualité.

275.Au plan interne, le Cil permet d'accompagner l'application des nouvelles règles de fond et des dispositions transitoires posées par la nouvelle loi. En outre, il permet d'organiser une communication entre les services et lui-même.

276.Au plan externe, le correspondant peut constituer un avantage pour répondre aux plaintes du personnel et des personnes concernées.

277.Sa désignation favorise également le dialogue avec la Cnil.

278.A cet égard, la mise en place des meilleures pratiques pourrait être favorisée par la création d'un réseau de correspondants afin de favoriser les échanges d'information entre les Cils ainsi que la formation et la protection de ces derniers.

279.Dans cette perspective, une première étape a d'ores et déjà été franchie avec la création de l'Association Française des Correspondants à la protection des Données à caractère Personnel (AFCDP).

[127] Art. 27, II de la loi Informatique et libertés modifiée.
[128] Art. 226-16 du C. pén.
[129] Art. 226-16 A du C. pén.
[130] Art. 226-16 A du C. pén.

6.2.2 La désignation

280.Sur le plan organisationnel, la loi ne précise pas le caractère interne ou externe de la fonction de Cil. De même, elle ne précise pas si le Cil est une personne physique ou une personne morale.

281.Dès lors, il semble que le responsable du traitement puisse désigner un correspondant externe[131], qui pourrait être une personne physique ou une personne morale.

282.Dans ce dernier cas, des prestataires de service, des avocats ou des experts comptables pourraient exercer la fonction de Cil.

283.Le décret d'application du 20 octobre 2005 apporte des précisions quant aux procédures de désignation et de révocation du correspondant à la protection des données à caractère personnel ; le décret apporte également des précisions sur la personne du correspondant, sa mission, ses attributions et ses obligations.

284.Sur la désignation du correspondant :

- la forme et le contenu de la notification de la désignation du correspondant auprès de la Cnil est précisée laquelle doit être précédée d'une autre notification auprès de l'instance représentative du personnel compétente, par lettre recommandée avec demande d'avis de réception par le responsable du traitement ;

- le correspondant peut-être externe à l'entreprise uniquement si moins de 50 personnes sont chargées de la mise en œuvre ou ont accès au traitement automatisé ;

- un correspondant unique peut être désigné dans le cadre de sociétés soumises à un même contrôle, d'un GIE ou encore d'organismes professionnels au sein d'un même secteur d'activité ;

- le responsable du traitement automatisé ou son représentant légal ne peut-être lui-même désigné correspondant à la protection des données ;

- les fonctions du correspondant au sein de l'entreprise ne doivent « pas être susceptibles de provoquer un conflit d'intérêt avec sa mission » et le correspondant ne doit recevoir « aucune instruction pour l'exercice de sa mission ».

285.La désignation d'un Cil pourrait, dans l'avenir proche, devenir obligatoire.

286.Une proposition de loi, déposée au Sénat le 6 novembre 2009[132], et récemment votée en première lecture au Sénat prévoit de rendre obligatoire la désignation de Cils lorsqu'une autorité publique ou un organisme privé recourt à un traitement de données à caractère personnel et que plus de 50 personnes y ont directement accès ou sont chargés de sa mise en œuvre.

287.Ce projet prévoit la possibilité pour la Cnil d'exercer le pouvoir de sanction que lui confère l'article 45-I de la loi Informatiques et liberté en cas de non-respect de cette obligation.

[131] Voir Alain Bensoussan, « Le correspondant à la protection des données à caractère personnel : un maillon important de la réforme », Gaz. Pal. nos 284 à 285 du 10 au 12-10-2004, p. 7 et s.
[132] Proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique, Doc. Sénat n°93 du 6-11-2009.

288.L'article 35 de la proposition de règlement européen du 25 janvier 2012[133] fait obligation au responsable de traitement et au sous-traitant de désigner un « délégué à la protection des données » lorsque :

- le traitement est effectué par une autorité ou un organisme publics ; ou
- le traitement est effectué par une entreprise employant au moins 250 personnes, ou
- les activités de base du responsable du traitement ou du sous-traitant consistent en des traitements qui, du fait de leur nature, de leur portée et/ou de leurs finalités exigent un suivi régulier et systématique des personnes concernées.

289. Par ailleurs, la proposition de règlement européen sur la protection des données adoptée par la Commission des libertés civiles, de la justice et des affaires intérieures, adoptée le 21 octobre 2013, rend obligatoire la désignation d'un délégué à la protection des données pour les entreprises traitant les données de plus de 5000 personnes physiques par an.

6.2.3 Les missions

290.En contrepartie de l'exemption des formalités préalables, le Cil se voit confier une double mission.

291.Une première mission consiste à encourager un contrôle interne afin que l'utilisation des données personnelles soit mise en œuvre de manière citoyenne.

292.A cette fin, le Cil dispose d'une large indépendance pour vérifier si les traitements opérés par le responsable du traitement sont conformes aux obligations légales, notamment en termes d'usage et de sécurité.

293.Dans cette perspective, le Cil devra lors de sa prise de fonction adresser un inventaire, c'est-à-dire auditer la situation, mettre en place les procédures éventuelles de régularisation, définir des points de contrôle et organiser une communication entre les services et lui-même afin de pouvoir assurer les fonctions qui lui incombent personnellement.

294.La seconde mission du Cil est d'établir la liste exhaustive des traitements « immédiatement » accessible à toute personne qui en fait la demande. Sa maintenance pour les opérations de création, de modification ou de suppression est faite à l'initiative du correspondant après information des services concernés.

295.La loi ne donne aucune autre précision sur les caractéristiques de cette liste.

296.Sur les missions du correspondant, le décret du 20 octobre 2005 prévoit que :

- dans les trois mois de sa désignation, il dresse une liste des traitements automatisés dont il devra délivrer une copie à toute personne qui en fait la demande ;

- il veille au respect des obligations prévues par la loi Informatique et libertés et, pour ce faire : il peut faire des recommandations au responsable des traitements ; il est consulté avant la mise en œuvre de tout traitement ; il reçoit les demandes et réclamations des personnes concernées par le traitement ; il informe le responsable des traitements de tout manquement avant, le cas échéant, de saisir la Cnil ; il réalise un bilan annuel de ses activités qu'il présente au responsable des traitements et qu'il tient à la disposition de la Cnil.

[133] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_fr.pdf

297.Le responsable des traitements a l'obligation de fournir au correspondant tous les éléments lui permettant d'établir et d'actualiser régulièrement la liste des traitements automatisés mis en œuvre au sein de l'établissement, du service ou de l'organisme au sein duquel il a été désigné.

298.Le correspondant a la faculté de saisir la Cnil concernant toute difficulté rencontrée dans l'exercice de ses missions.

299.Quant à la révocation du correspondant, celui-ci peut-être révoqué s'il a manqué aux devoirs de sa mission ; la procédure de révocation peut-être à l'initiative de la Cnil ou du responsable du traitement. La révocation devra répondre à un certain formalisme décrit par le décret d'application de la loi Informatique et libertés.

6.2.4 La responsabilité

300.Agissant en toute indépendance dans le cadre de sa mission, le Cil ne « peut faire l'objet d'aucune sanction de la part de l'employeur du fait de l'accomplissement de ses missions ».

301.En cas de difficulté, il peut saisir la Cnil des difficultés qu'il rencontre dans l'exercice de ses missions.

302.Cette saisine peut se faire par tout moyen.

303.En cas de « manquement constaté à ses devoirs », le responsable du traitement peut décharger le Cil de ses fonctions sur demande, ou après consultation, de la Cnil.

304.Le responsable du traitement pourra alors soit désigner un nouveau Cil et mettre en œuvre la procédure de notification et d'information, procéder aux formalités préalables.