Jean Massot
Président de Section honoraire au Conseil d'Etat

LE CONTRÔLE DE L'ADMINISTRATION PAR UNE AUTORITÉ ADMINISTRATIVE INDÉPENDANTE : LA COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

UDK: 351 (44)
Izvorni znanstveni rad
Primljeno: 15. IX. 2015.

Le législateur français a créé en 1978 la première autorité administrative indépendante pour contrôler l'activité des pouvoirs publics, puis progressivement des opérateurs privés, en matière de recours à l'informatique pour traiter les données personnelles des citoyens.

La CNIL autorité administrative est bien indépendante du gouvernement et du parlement comme le montrent sa composition et son mode de fonctionnement. Elle reste contrôlée par le juge constitutionnel, administratif et judiciaire.

Elle assure le respect d'un certain nombre de principes aujourd'hui communs à toutes les autorités similaires de l'U.E.

Pour cela, elle exerce en premier lieu des contrôles a priori sur les décisions de création des traitements de données personnelles d'autant plus poussés que ces traitements présentent des risques pour les libertés.

Mais de plus en plus, elle développe des contrôles a posteriori, soit à la demande des citoyens, soit de sa propre initiative, qui peuvent aller jusqu'au prononcé de sanctions contre les responsables de traitement

Mots - clés*: Contrôle de l'administration, Commision nationale de l'informatique et des libertés, France*

INTRODUCTION

Le développement de l'informatique dans les années 1960-70 a d'abord concerné les administrations et les très grandes entreprises, seules en mesure de supporter le coût et l'encombrement des premiers matériels. Dès cette époque, les administrations qui détenaient depuis longtemps des fichiers « papier » regroupant les données personnelles des citoyens sous divers aspects (Etat civil, Impôts, Santé, Sécurité sociale, Justice, Police, Cadastre etc.) ont vu l'intérêt que présentait pour elles le traitement informatique de ces données. Cela leur était d'autant plus facile que tous les citoyens français sont dotés à leur naissance d'un numéro à treize chiffres, invariable et utilisé depuis longtemps par la sécurité sociale[1].

[1] D'où son appellation courante de « Numéro de sécurité sociale » alors que son appellation officielle est « Numéro d'inscription au répertoire nationale d'identification des personnes physiques », d'où sa seconde appellation courante de NIR.

Au début des années 1970, un projet a vu le jour sous le nom malencontreux de projet SAFARI[2]. Il s'agissait, par l'usage de ce numéro dans tous les fichiers administratifs préalablement informatisés, d'en permettre l'interconnexion généralisée. Ce projet suscita une grande émotion, certains redoutant une surveillance universelle de la population. On évoqua « Big Brother » et le livre d'Orwell « 1984 ». On prêta à l'ancien vice-président du Conseil d'Etat, Alexandre Parodi[3], la remarque selon laquelle avec un tel système pendant la guerre, la Résistance aurait été rapidement repérée et démasquée par la Gestapo. Ces craintes étaient avivées par le fait que le NIR avait malheureusement été initialement imaginé pour les besoins du recrutement militaire à la veille de la seconde guerre mondiale, puis développé sous l'occupation allemande. Or ce numéro, loin d'être aléatoire, est par lui-même « signifiant », puisqu'il est constitué de données indiquant le sexe, l'année, le mois, le département et la commune de naissance et que l'on peut facilement remonter à l'identité du porteur, au moins pour les petites communes. Certains en concluaient, heureusement à tort, qu'il avait servi à la traque des juifs sous le régime de Vichy, alors que, bien entendu, dans un Etat laïc comme la France, il n'a jamais comporté d'indications sur la religion ou la race[4]. Un article retentissant fut publié le 21 mars 1974 dans le journal « Le Monde » par Philippe Boucher sous le titre « SAFARI ou la chasse aux Français ». Devant cette émotion, le gouvernement chargea une commission de hauts magistrats, d'avocats et d'universitaires de proposer une solution. Ces travaux aboutirent à la loi du 6 janvier 1978 créant la Commission Nationale de l'Informatique et des Libertés ou CNIL, autorité administrative indépendante chargée d'éviter l'utilisation abusive des données informatisées propres aux citoyens.

Depuis lors, beaucoup de pays européens ont imité la France[5] en se dotant de textes et d'organes protecteurs des données personnelles. Ils y sont même tous contraints depuis l'adoption de la Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995[6], transposée en France par une loi du 6 août 2004 modifiant celle de 1978. Cette directive et les lois nationales seront bientôt remplacées par un règlement communautaire en discussion depuis janvier 2012 qui devrait aboutir en 2016.

Il faut bien sûr garder en mémoire que le développement de la micro-informatique et de l'internet a depuis longtemps mis fin au monopole des grandes structures publiques et privées et qu'aujourd'hui tout le monde est susceptible de traiter les données personnelles des autres et se trouve devoir respecter les principes de la loi Informatique et libertés. Même si ce que je vais exposer

[2] Les informaticiens adorent les acronymes : celui-ci voulait représenter « **S**ystème **A**utomatisé pour les **F**ichiers **A**dministratifs et le **R**épertoire des **I**ndividus ».

[3] Grand résistant, il avait été le délégué du général De Gaulle pour la Libération de Paris.

[4] Sauf pendant une très brève période du régime de Vichy en Algérie. Bien entendu, il y eut hélas des fichiers manuels des juifs, mais ils ne comportaient pas ce numéro.

[5] Qui n'avait été devancée que par certains Länder allemands et la Suède.

[6] Le chapitre VI de la directive est consacré à l'Autorité de contrôle que chaque Etat membre est appelé à mettre en place.

serait donc aussi valable pour les plus petits opérateurs privés, ce n'est qu'à la présentation de ce mode de contrôle très particulier de **l'administration** par une autorité administrative indépendante ou AAI qu'est consacrée ma contribution[7]. Je le ferai en exposant successivement

1) En quoi la CNIL est une autorité administrative indépendante,
2) Quels sont les principes au respect desquels elle doit veiller,
3) Quels sont ses moyens de contrôle a priori,
4) Quels sont ses moyens de contrôle a posteriori.

I. LA CNIL AUTORITÉ ADMINISTRATIVE INDÉPENDANTE

Dès la création de la CNIL par la loi du 6 janvier 1978 sous l'appellation nouvelle d'autorité administrative indépendante ou AAI[8], beaucoup de bons esprits ont souligné la contradiction apparente entre les adjectifs « administrative » et « indépendante ». La Constitution de 1958 ne dit-elle pas à son article 20 que le gouvernement « dispose de l'administration », ce qui est la consécration du pouvoir hiérarchique dont disposent les membres du gouvernement sur les services qui leur sont rattachés, à moins que, disposant de la personnalité morale, ces services ne soient soumis qu'à une simple tutelle ministérielle. Or, précisément, la CNIL n'a pas la personnalité morale. La loi de 1978 dispose pourtant en son actuel article 21 que « dans l'exercice de leurs attributions, les membres de la commission ne reçoivent d'instructions d'aucune autorité » et qu'au contraire « les ministres et autorités publiques ne peuvent s'opposer à l'action de la commission et doivent prendre toutes mesures utiles pour favoriser sa tâche ». Certains se sont donc interrogés à l'époque sur la constitutionnalité de ce système. Mais la loi de 1978 n'avait pas été soumise au Conseil constitutionnel[9]. Il fallut donc attendre plusieurs années pour que la constitutionnalité de ce mode très particulier de contrôle de l'administration fût consacrée à propos d'une autre AAI, l'autorité administrative de garantie de l'indépendance de l'audiovisuel public[10]. Le Conseil constitutionnel prit soin de rappeler que si les dispositions de l'article 21 de la Constitution confient au Premier ministre l'exercice du pouvoir réglementaire, « ces dispositions ne font cependant pas obstacle à ce que le législateur confie à une autorité de l›État autre que le Premier ministre, le soin de fixer, dans un domaine déterminé et dans le cadre défini par les lois et règlements, des normes permettant de mettre en œuvre une loi ». Mais il censura la possibilité de subordonner l'édiction de décrets à l'avis favorable ou la proposition d'une AAI. On y reviendra à propos de la CNIL.

---

[7] J'ai été membre de cette autorité de 2005 à 2014

[8] La CNIL a fait école : il existe aujourd'hui une bonne quarantaine de ces autorités.

[9] Et, à l'époque, il n'existait pas de contrôle a posteriori de la constitutionnalité.

[10] Décision n°86-217 du 18 septembre 1986

Quoi qu'il en soit, l'indépendance de la CNIL est consacrée par diverses dispositions.

En premier lieu, le collège de dix-sept membres qui est l'instance de décision ne comprend qu'une très petite part de personnalités nommées par le gouvernement[11] : trois seulement, encore doivent-elles être qualifiées par leur connaissance de l'informatique ou des questions touchant aux libertés individuelles. Les autres sont six hauts magistrats désignés par le Conseil d'Etat[12], la Cour de cassation et la Cour des comptes, six parlementaires désignés par l'Assemblée nationale, le Sénat[13] et le Conseil économique, social et environnemental et enfin deux personnalités qualifiées par leur connaissance de l'informatique désignées par les présidents de l'Assemblée nationale et du Sénat.

Il faut ajouter que c'est ce collège qui élit en son sein un président et deux vice-présidents ainsi que la formation restreinte qui sera appelée à prononcer les sanctions, comme nous le verrons. La preuve que ce mode de désignation est bien un gage d'indépendance a été apportée par la dernière élection, celle en 2014 de la présidente actuellement en fonctions : membre du Conseil d'Etat, elle l'a emporté sur un autre candidat qui, lui, avait été nommé par le gouvernement.

Tous ces membres doivent informer le président de la Commission des intérêts qu'ils détiennent ou viennent de détenir dans une personne morale, Etat, collectivité ou établissement public, entreprise privée, et s'abstenir de participer aux délibérations touchant à de tels intérêts.

Le mandat des membres du collège ne peut être interrompu que par un décès, une démission ou la constatation par la Commission elle-même de trois absences successives non justifiées.

Enfin, si le gouvernement est représenté aux séances de la Commission par un « commissaire du gouvernement », ce dernier n'a d'autre prérogative que d'être informé à l'avance des projets qui seront soumis au vote du collège et de faire valoir le point de vue du gouvernement lors de la séance, mais avec une voix simplement consultative[14].

Cette indépendance des autorités de protection des données personnelles est aujourd'hui consacrée au niveau européen par l'article 28.1 de la directive déjà évoquée. La Cour de Justice de l'Union a été amenée à censurer l'insuffisante indépendance des autorités de contrôle des Länder allemands, comme de celles de l'Autriche et de la Hongrie.[15] Bien entendu, l'indépendance ne signifie pas que la CNIL échappe à tout contrôle ; ses délibérations, quand elles ont une portée

[11] Qui pourtant en vertu de l'article 21 de la Constitution nomme aux emplois civils et militaires.

[12] Ce fut mon cas de 2005 à 2014.

[13] En assurant, pour ces deux assemblées politiques, une représentation pluraliste, soit un de la majorité et un de l'opposition.

[14] Il peut théoriquement imposer une nouvelle délibération dix jours plus tard. Je n'ai jamais vu faire usage de cette prérogative.

[15] Respectivement, 9 mars 2010, Commission et Contrôleur européen de protection des données personnelles c/RFA, 16 octobre 2012, les mêmes c/Autriche et 8 avril 2014 les mêmes c/Hongrie

normative, sont soumises au contrôle du juge administratif, qui veille notamment à ce que, dans son contrôle sur l'administration, l'autorité administrative indépendante ait une juste appréciation des principes qu'elle doit faire respecter. Ces principes, quels sont-ils ?

II. L'OBJET DU CONTRÔLE : LE RESPECT DES PRINCIPES DE LA LOI INFORMATIQUE ET LIBERTÉS

Comme je l'ai indiqué, la loi, conçue initialement pour encadrer les traitements informatiques de l'administration, s'applique à tous les opérateurs qui traitent des données personnelles[16]. Mais certains des principes qu'elle pose font l'objet d'adaptations aux besoins du service public et à la nécessité de concilier les droits de l'Etat avec les droits privés, selon l'adage fondateur du droit administratif[17].

J'exposerai donc successivement les droits « indérogeables », c'est-à-dire ceux qui s'imposent à tous, avant de décrire ceux qui font l'objet d'adaptations lorsque sont en cause des opérateurs publics.

Les règles auxquelles nul ne peut déroger se trouvent principalement aux articles 6 de la directive de 1995 et de la loi dans sa version modifiée en 2004 pour transposer la directive.

Il s'agit d'abord de l'obligation de collecter et traiter les données de manière loyale et licite, ce qui se comprend par soi-même : le piratage est évidemment interdit, sauf si un texte de loi le permet pour les services de renseignement.

Il s'agit ensuite du principe de finalité qui veut que le responsable du traitement fasse connaître le but dans lequel les données personnelles sont collectées et qu'il se limite et se tienne à ce but, sous réserve d'une utilisation ultérieure à des fins de recherche historique ou scientifique.

Puis vient le principe de proportionnalité, en vertu duquel le responsable du traitement ne doit collecter et traiter que ce qui est nécessaire pour atteindre les buts qu'il a énoncés. En complément, ce traitement doit être limité dans le temps au regard des mêmes nécessités. La justice et la police ne peuvent conserver les données d'infractions que pour une durée limitée.

Enfin, les données doivent être exactes, complètes et, si nécessaire, mises à jour.

L'article 6 est complété par une disposition traditionnelle selon laquelle aucune décision produisant des effets juridiques à l'égard d'une personne ne peut avoir pour seul fondement un traitement automatisé de données à caractère personnel : l'homme doit toujours pouvoir garder le pouvoir de s'écarter de ce que lui indique

[16] La loi, dans sa version initiale, parlait d'informations nominatives : la terminologie actuelle dans sa version complète est « données à caractère personnel », transposition de la directive de 1995 qui, dans sa version anglaise, parle plus sobrement de « personal data ».

[17] Arrêt du Tribunal des conflits « Blanco » du 8 février 1873.

la machine, transposition moderne du vieux principe de l'examen individuel, imposé depuis longtemps à l'administration par la jurisprudence.

Les règles auxquelles des dérogations sont prévues en faveur des opérateurs publics et de certains opérateurs privés sont également nombreuses. Le caractère commun de ces dérogations est le plus souvent de faire intervenir la CNIL.

C'est en premier lieu le cas de la règle traditionnelle selon laquelle « il est interdit de collecter ou de traiter des données à caractère personnel 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 ». Bien entendu, il existe, pour les premières, une dérogation en faveur des organismes[18] à but non lucratif et à caractère religieux, philosophique, politique ou syndical et pour l'avant dernière, la santé, en faveur des traitements médicaux que les opérateurs soient publics ou privés. Mais il existe aussi une dérogation plus générale pour les « traitements justifiés par l'intérêt public », à condition qu'ils soient autorisés par la CNIL dans des conditions sur lesquelles je reviendrai.

C'est le cas ensuite de la règle selon laquelle « Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée », car le texte ajoute immédiatement « ou satisfaire à l›une des conditions suivantes 1° Le respect d›une obligation légale incombant au responsable du traitement….

3° L›exécution d›une mission de service public dont est investi le responsable ou le destinataire du traitement….

5° 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. » On conçoit que la police, la justice ou le fisc remplissent les conditions 1 et 3. Néanmoins, il appartient à la CNIL de le vérifier au cas par cas.

De la même façon, le principe posé au premier alinéa de l'article 38 de la loi selon lequel « 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 » est aussitôt atténué par le troisième alinéa selon lequel « les dispositions du premier alinéa ne s'appliquent pas lorsque le traitement répond à une obligation légale ou lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte autorisant le traitement ». On conçoit que le délinquant, voire le contribuable, ne soit pas autorisé à s'opposer au traitement de ses données par la justice, la police ou le fisc. Il appartient là encore à la CNIL de vérifier que les conditions légales sont remplies.

Corollaires du droit précédent, les article 39 et 40 ouvrent à toute personne un droit d'accès au traitement de ses données personnelles et un droit d'exiger du responsable du traitement la correction d'inexactitudes, voire l'effacement de données périmées. Mais l'article 41 crée immédiatement, pour les traitements qui

[18] Eglises, partis politiques, syndicats, associations.

intéressent la sûreté de l'Etat, la défense ou la sécurité publique, une procédure de droit d'accès plus limitée, puisqu'elle passe par l'intervention d'un des magistrats membre de la CNIL qui se rend auprès du responsable du traitement pour décider avec lui[19] si les données peuvent être communiquées et si elles doivent être rectifiées dans des conditions variables selon le caractère plus ou moins sensible du traitement : dans certains cas, notamment pour les fichiers de terrorisme, le demandeur peut même ne pas être informé du point de savoir s'il y figure ou non.

Un cas très particulier est celui des traitements de données à caractère personnel relatives « aux infractions, condamnations et mesures de sûreté ». L'article 9 de a loi n'en permet en effet la mise en œuvre que par « les juridictions, les autorités publiques et les personnes morales gérant un service public, agissant dans le cadre de leurs attributions légales » et « par les auxiliaires de justice, pour les stricts besoins de l›exercice des missions qui leur sont confiées par la loi »[20]. On verra que la création de tels traitements est soumise à une procédure stricte qui fait intervenir la CNIL.

Si, enfin, l'article 68 de la loi dispose que « le responsable d'un traitement ne peut transférer des données à caractère personnel vers un Etat n'appartenant pas à la Communauté (sic) européenne que si cet Etat assure un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l›égard du traitement dont ces données font l›objet ou peuvent faire l›objet », l'article suivant dispense de cette vérification les traitements nécessaires à la sauvegarde de l'intérêt public. Mais, là encore, si la création de ce traitement doit lui être soumise, ce qui sera très généralement le cas, la CNIL vérifiera que ce transfert ne présente pas de risques excessifs.

Pour conclure cette partie, on peut retenir que, si les traitements de données à caractère personnel des autorités publiques bénéficient de larges dérogations aux principes généraux de la protection de ces données, ce n'est qu'au bénéfice d'un contrôle strict de la CNIL lors de la création de ces traitements. C'est tout l'objet des contrôles a priori dont on va parler maintenant.

III. LES CONTRÔLES « A PRIORI »

Lors de l'adoption de la loi de 2004 transposant la directive de 1995, on a souvent relevé que les pouvoirs de contrôle a priori avaient diminué au profit des contrôles « ex post ». Il est vrai que la philosophie du texte communautaire[21] est de mettre en avant la simple déclaration des traitements à l'autorité de contrôle, ne lui permettant ainsi que des contrôles a posteriori. Il faut toutefois relever qu'en fonction des compétences communautaires de l'époque, la directive ne s'appliquait pas aux traitements ayant pour objet la sécurité publique, la défense et la sécurité

[19] Ce qui veut bien dire qu'il faut l'accord et du magistrat et du responsable du traitement.

[20]

[21] Et ce sera encore plus vrai du futur règlement qui privilégiera l' « accountability », c'est-à-dire l'obligation de rendre compte a posteriori.

de l'Etat, dont on va voir qu'ils sont précisément ceux qui mobilisent les pouvoirs de contrôle a priori les plus importants de la CNIL[22]. Il reste vrai néanmoins que ces pouvoirs ont, depuis 2004, diminué en intensité. Pour le comprendre, il faut entrer dans le détail des formalités qui s'imposent à tout responsable de traitement avant de procéder à sa mise en œuvre.

Le plus bas niveau est celui de la dispense de toute formalité qui peut résulter directement de la loi elle-même : c'est le cas des traitements « ayant pour seul objet la tenue d'un registre qui, en vertu de dispositions législatives ou réglementaires, est destiné exclusivement à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime » : cela vise par exemple les annuaires. C'est aussi le cas des traitements pour lesquels le responsable a désigné un « correspondant à la protection de données personnelles » ou « correspondant Informatique et libertés (CIL) », institution inspirée de l'expérience allemande[23] et qui a la charge de veiller en interne au respect de la loi. C'est enfin le cas des traitements pour lesquels la CNIL décide de les dispenser de la formalité la plus simple qu'est la déclaration : aujourd'hui sont en vigueur 18 délibérations édictant de telles dispenses et s'appliquant à des sujets aussi variés que la gestion des rémunérations, comme des œuvres sociales et culturelles, la tenue du fichier électoral des communes, la consultation du cadastre ou la gestion administrative, comptable et pédagogique des établissements d'enseignement secondaire publics et privés.

C'est aussi le cas pour les traitements pour lesquels la CNIL fait usage de son pouvoir d'édicter une « norme simplifiée » (NS) qui précise les obligations du responsable de certains traitements non susceptibles de porter atteinte à la vie privée ou aux libertés, donc les moins dangereux, et qui permet à ce responsable de souscrire simplement un engagement de se conformer à cette norme. On trouve de telles NS dans des domaines tels que l'état-civil ou le recouvrement des impôts. Mais de très nombreux traitements des autorités publiques continuent de relever, après comme avant 2004, de procédures plus lourdes qui sont décrites aux articles 25 à 27 de la loi. La formalité classique est alors l'autorisation du traitement par décret en Conseil d'Etat pris après avis motivé et publié de la CNIL. Elle s'applique aux traitements mis en œuvre par l'Etat qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique ainsi qu'aux traitements d'infractions pénales, dès lors que ces traitements portent sur des données sensibles, celles dont la collecte est en principe interdite comme on l'a vu plus haut (origines raciales ou ethniques, opinions, santé, mœurs)[24]. C'est aussi le cas des traitements

[22] Le projet de règlement n'en traitera pas. Ils feront l'objet d'une nouvelle directive.

[23] Qui sera sans doute généralisée par le règlement au moins pour les opérateurs d'une certaine taille.

[24] Si ces données sensibles ne sont pas en cause, le décret sur le pouvoir réglementaire des AAI en Conseil d'Etat est remplacé par un arrêté ministériel.

mis en œuvre par l'ensemble des services publics[25] dès lors qu'ils portent sur le NIR ou sur des données biométriques[26].

C'est ici que bon nombre d'observateurs ont pu déceler une diminution des pouvoirs de la CNIL. En effet, dans la version initiale de la loi de 1978, tous les traitements des opérateurs publics devaient faire l'objet d'un acte réglementaire pris après avis de la CNIL[27], et si cet avis était défavorable, il ne pouvait être passé outre que par un décret pris sur avis conforme du Conseil d'Etat. Bien plus, dans le cas des traitements de données sensibles, il fallait un décret en Conseil d'Etat pris sur proposition ou avis conforme de la CNIL. La vérité est que, sous l'empire de ces dispositions, le gouvernement n'allait jamais jusqu'à l'avis défavorable de la CNIL, mais négociait avec elle jusqu'à obtenir un texte de compromis : ce fut le cas par exemple pour l'utilisation d'un numéro d'identification des contribuables, dont la CNIL obtînt qu'il ne fût pas le NIR. La vérité est aussi, hélas, que certains traitements sensibles, notamment ceux de la police ou des services de renseignement, furent pendant longtemps mis en œuvre sans aucune intervention de la CNIL.

La CNIL a donc perdu ce pouvoir de blocage au profit d'un simple avis rendu public. Il ne faut pas pour autant minimiser la portée de cet avis : l'expérience récente a montré que cet avis avait pu, dans certaines hypothèses, convaincre le gouvernement de faire machine arrière et dans d'autres, influer sur la décision contentieuse du juge administratif saisi. Ce fut le cas récemment par exemple sur le nombre de doigts dont on recueille les empreintes pour établir le passeport électronique (Assemblée 26 octobre 2011 n°317827) : le Conseil d'Etat a donné raison à la CNIL qui, par application du principe de proportionnalité, avait estimé que deux doigts suffisaient, alors que le gouvernement avait prévu de collecter les empreintes des dix doigts.

En ce qui concerne l'avis conforme ou le pouvoir de proposition dont la CNIL disposait pour le traitement des données sensibles, il est sans doute vain de le regretter, car si la version initiale de la loi de 1978 n'avait pas été soumise au Conseil constitutionnel, ce dernier, à l'occasion de l'examen d'une loi plus récente qui redonnait un tel pouvoir à la CNIL, a estimé que cet empiètement sur le pouvoir réglementaire du Premier ministre dépassait les limites qu'il avait fixées par ses décisions précitées sur le pouvoir réglementaire des AAI et il a censuré le mot « conforme » (Voir la décision 2006-544 DC du 14 décembre 2007). La disposition initiale de la loi n'aurait sans doute pas résisté à une nouvelle saisine du Conseil par la procédure de question prioritaire de constitutionnalité.

Mais il existe un domaine où les pouvoirs de la CNIL connaissent une limitation supplémentaire, c'est celui de certains traitements intéressant la sûreté de l'Etat, la défense ou la sécurité publique qui peuvent être dispensés de publication par

[25] Donc non seulement ceux de l'Etat, mais aussi des collectivités territoriales, des établissements publics, voire des organismes privés chargés de la gestion d'un service public.

[26] Empreintes digitales ou de manière plus moderne, empreintes génétiques (ADN).

[27] Sous réserve de l'application d'une norme simplifiée.

un décret en Conseil d'Etat et pour lesquels n'est publié, en même temps que le décret les dispensant de publication, que le sens de l'avis de la CNIL sans aucun élément de son argumentaire. Il s'agit essentiellement des traitements des quatre grands services civils et militaires de renseignement intérieur et extérieur.

Il faut enfin noter une limitation supplémentaire des pouvoirs de contrôle a priori de la CNIL : c'est le cas où le gouvernement décide de recourir au législateur pour la création de traitements sensibles. Certes, la CNIL doit être consultée sur les projets de loi relatifs à la protection des personnes à l'égard des traitements automatisés. Certes aussi le président de toute commission parlementaire peut demander la publication de son avis : c'est ce qui s'est fait pour la loi sur le renseignement adoptée avant l'été (Voir sur le site de la CNIL la délibération n°2015-078 du 5 mars 2015). Mais on sait bien qu'entre le projet initial soumis à la CNIL[28] et le texte soumis au vote parlementaire, de nombreux amendements peuvent en altérer sensiblement la portée et pas toujours dans un sens favorable à la protection des libertés.

Le dernier et le plus important pouvoir de contrôle a priori de la CNIL est celui d'autoriser ou non les traitements. Certes, ce pouvoir n'existe que pour les traitements qui ne relèvent pas de l'autorisation par décret ou arrêté, comme ceux dits de souveraineté (sûreté de l'Etat, défense, sécurité publique) ou ceux qui traitent le NIR ou des données biométriques. Cela laisse encore un champ d'intervention non négligeable, en particulier lorsqu'il y a traitement de données sensibles en dehors de ces domaines : pour citer un domaine dont je me suis beaucoup occupé, je citerai la mise en ligne des archives d'état-civil[29]. La CNIL recourt alors souvent, lorsqu'il s'agit de traitements identiques mis en œuvre par des responsables différents[30], à la procédure de l'autorisation unique (AU) qui n'oblige les responsables qu'à souscrire un engagement de conformité.

Mais, en tout état de cause, les pouvoirs de la CNIL sont renforcés par l'existence de contrôles a posteriori.

IV. LES CONTRÔLES « A POSTERIORI »

On peut en présenter trois catégories : en premier lieu, l'exercice du droit d'accès indirect, ensuite les contrôles sur place et enfin les sanctions.

Je rappelle que le droit d'accès indirect s'applique aux traitements intéressant « la sûreté de l'Etat, la défense ou la sécurité publique » pour lesquels la personne qui se croit concernée ne peut directement vérifier les informations contenues dans les fichiers et doit s'adresser à la CNIL. Celle-ci désigne alors un de ses membres magistrats pour se rendre auprès du responsable du traitement et

[28] Et d'ailleurs au Conseil d'Etat.

[29] Dont beaucoup de données touchent à la vie privée.

[30] Comme les services départementaux des archives

se mettre d'accord avec lui sur les suites à donner à la demande. L'issue de la procédure varie considérablement selon les traitements en cause.

Pour les traitements les moins sensibles, tels que ceux d'informations générales sur les mouvements politiques, religieux ou syndicaux et leurs manifestations[31], la procédure conduit en cas d'accord entre le responsable du traitement et le magistrat de la CNIL à communiquer tout ou partie du fichier à l'intéressé qui peut alors faire verser au dossier ses propres observations contestant tel ou tel point.

Pour les traitements de la police dits d' « antécédents judiciaires » ou TAJ[32] qui retracent toutes les mises en cause du fait d'une possibilité d'infraction, la procédure conduit très souvent à des rectifications sur lesquelles les deux parties se mettent facilement d'accord, soit parce que les durées de conservation sont expirées, soit parce que la procédure judiciaire n'a pas abouti à une condamnation et que cette information n'est pas remontée du parquet vers les services de police.

Le rôle de la CNIL est, ici, d'autant plus utile que ces rectifications imposées par la loi sont malheureusement très fréquentes. L'inconvénient et que ces rectifications prennent souvent beaucoup de temps.

Pour les traitements les plus sensibles, ceux des services en charge de lutter contre le terrorisme ou le blanchiment d'argent, la procédure est beaucoup moins favorable aux intéressés, dans la mesure où ils sont seulement informés qu'une vérification a été faite, mais nullement de son issue. Les services de renseignement s'opposent même à ce que les intéressés soient informés du point de savoir s'ils figurent ou non dans le fichier. Cette question fait actuellement l'objet d'un contentieux qui est remonté jusqu'au Conseil d'Etat : le juge administratif peut-il avoir connaissance du contenu de ces fichiers sans qu'il soit soumis au contradictoire ?

Enfin, pour les fichiers Schengen, il y a une combinaison des diverses solutions ci-dessus exposées selon les motifs des signalements qui justifient un refus d'accès au territoire : simple information que les vérifications ont été faites en cas de surveillance discrète pour prévenir les menaces à la sécurité publique, rectifications en accord avec l'Etat à l'origine du signalement si les motifs du signalement sont caducs ou erronés : une abondante jurisprudence du Conseil d'Etat renforce les pouvoirs et les obligations de la CNIL en la matière.

A côté de ces vérifications qui ne se font qu'à la demande d'une personne privée, la CNIL a, depuis l'origine, des pouvoirs généraux de contrôle qui lui permettent de se rendre auprès des responsables de traitement et de se faire communiquer tout document utile pour vérifier que ces traitements sont bien menés conformément à la loi. Beaucoup plus fréquents à l'égard des opérateurs privés que sur les traitements publics, ces contrôles n'en existent pas moins : la CNIL en a par exemple mené un en 2013 sur le fichier d'antécédents judiciaires de la police ou STIC.

---

[31] Ce que l'on appelait classiquement les Renseignements généraux ou « RG »

[32] Résultant de la fusion des fichiers STIC de la police et JUDEX de la gendarmerie

Enfin, soit à la suite de ces contrôles, soit sur une plainte d'un particulier, la CNIL peut être conduite à prononcer une sanction à l'encontre du responsable du traitement. La jurisprudence de la Cour européenne des droits de l'homme relayée par celle du Conseil d'Etat a conduit récemment à mieux distinguer l'autorité de poursuite, la présidence de la CNIL et l'autorité de jugement, une formation restreinte à laquelle les organes directeurs de la commission[33] n'appartiennent pas. De telles sanctions essentiellement pécuniaires, voire ordonnant la suspension du traitement, ne sont pas envisageables à l'encontre d'un service de l'Etat. En revanche, elles peuvent intervenir à l'encontre de collectivités territoriales et ne sont nullement exceptionnelles par exemple lorsque des services communaux « fichent » de manière illégale les habitants de cette collectivité.

CONCLUSION

L'existence d'une autorité administrative indépendante protégeant les données à caractère personnel est devenue un élément essentiel de la conception française de l'Etat de droit. Certains ont même pensé qu'il serait souhaitable de l'inscrire dans le préambule de la Constitution. Un rapport d'une commission présidée par Madame Simone Veil en 2008 et chargée d'étudier d'éventuels ajouts à ce préambule ne l'a pas proposé, dans la mesure où tant la jurisprudence constitutionnelle que les textes de l'Union européenne garantissent suffisamment cette modalité de contrôle de l'administration dans ce domaine capital. Certes tout n'est pas parfait et les nécessités de la lutte contre le terrorisme vont souvent au cela de ce que la CNIL souhaiterait. Mais c'est bien la jurisprudence constitutionnelle et européenne qui admet que la protection de la vie privée doit se concilier avec d'autres principes tels que la préservation de l'ordre public.

[33] Président et vice-présidents

KONTROLA UNPRAVE PUTEM JEDNOG NEZAVISNOG UPRAVNOG TIJELA: NACIONALNO POVJERENSTVO ZA INFORMATIKU I SLOBODE

Francuski zakonodavac je 1978. osnovao prvo nezavisno upravno tijelo za kontrolu aktivnosti javnih vlasti, zatim postupno i za kontrolu privatnih subjekata, pri uporabi računala za obradu osobnih podataka građana.

CNIL je upravno tijelo koje ne ovisi ni o vladi niti o parlamentu kao što to njegov sastav i način djelovanja potvrđuju. Ustavni, upravni i redovni sudac kontroliraju Nacionalno povjerenstvo za informatiku i slobode. Ono jamči poštivanje određenog broja načela koja su danas zajednička svim sličnim tijelima u Europskoj uniji.

Zbog toga, to povjerenstvo prvenstveno obavlja prethodne kontrole odluka o provođenju obrade osobnih podataka, a koje su još strože u slučaju da predstavljaju opasnost za slobode.

Međutim, povjerenstvo sve češće provodi naknadne kontrole na zahtjev građana ili samoinicijativno, a posljedica može biti izricanje kazni protiv odgovornih osoba za obradu podataka.

Ključne riječi: *Kontrola administracije, Nacionalno povjerenstvo za informatiku i slobode, Francuska*

CONTROL OF ADMINISTRATION BY AN INDEPENDENT ADMINISTRATIVE BODY: NATIONAL COMMISSION FORCOMPUTER TECHNOLOGY AND FREEDOMS

The French legislator in 1978 founded the first independent administrative body to control the activities of public authorities, then gradually to control private subjects with the use of the computer for analysing the personal data of citizens.

CNIL is an administrative body which is independent of the government or parliament as its constitution and method of activity confirm. Constitutional, administrative and regular judges control the National Board for computer technology and freedoms. It guarantees respecting a certain number of principles which are common to all similar bodies in the European Union.

Due to this, the Board mainly carries out previous controls of the decision on implementing analysis of personal data which are even stricter if it is a case of endangering freedom.

However, the Board more and more often carries out additional controls upon citizen request or of its own accord. The consequence can be sentencing the persons responsible for data analysis.

Key words: *Control of administration, National commision for information and freedoms, France*