

**DATENSCHUTZGRUNDVERORDNUNG UND IHRE DAGEGEN
GERICHTETEN RECHTBEHELFE VOR DEN
VERWALTUNGSGERICHTEN**

**LE REGLEMENT EUROPEEN 2016-679 DU 27 AVRIL 2016, SUR LA
PROTECTION DES *PERSONNES PHYSIQUES* A L'EGARD DU
TRAITEMENT DES DONNEES, ET LES RECOURS
JURIDICTIONNELS DEVANT LES TRIBUNAUX ADMINISTRATIFS**

**IL REGOLAMENTO EUROPEO, RELATIVO ALLA PROTEZIONE
DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO
DEI DATI PERSONALI, E I RICORSI DAVANTI ALLE
GIURISDIZIONI AMMINISTRATIVE**

Liebe Kolleginnen und Kollegen,

Cari colleghe e colleghi,

Chers collègues !

INTRODUCTION :

« L'informatique doit être au service de chaque citoyen. (...) Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ». Ces mots figurent à l'article 1^{er} de la **loi du 6 janvier 1978, dite loi « informatique et libertés »**. Comme le notait Jean Marc Sauvé, vice-président du Conseil d'Etat français jusqu'en mai dernier, ¹ il apparaît qu'en France, dès 1978, le législateur français s'est préoccupé des risques

¹ Septièmes entretiens du Conseil d'État en droit social : Santé et protection des données
Conseil d'État - Vendredi 1^{er} décembre 2017

que l'informatique peut faire peser sur les libertés fondamentales et, notamment, sur le respect de la vie privée.

Aujourd'hui, en 2018, le développement d'Internet a bouleversé les données du problème. En effet, avec l'essor d'Internet et des plateformes numériques, les données personnelles sont devenues la matière première de l'activité des géants du Web, *die sogennante GAF*A (=GOOGLE, Apple, Facebook et Amazone), et des réseaux sociaux. D'une part, il faut essayer de faciliter cette circulation d'information, sans y mettre des entraves excessives, mais d'autre part il faut maintenir l'objectif de préserver les libertés des citoyens, *« dont les données peuvent être erronées, collectées et conservées de manière injustifiée ou disproportionnée et, de surcroît, sont susceptibles de révéler, sur chaque personne, des habitudes, des préférences ou des opinions² »*. A cet effet, le rôle du juge en général, et du juge administratif en particulier, qui entend maintenir en France sa place en tant que protecteur des libertés, est essentiel. Telle est la philosophie du Règlement européen qui vient d'entrer en vigueur le 25 mai 2018.

I HISTORIQUE : de 1978 à 2018

C'est avec la **loi du 6 janvier 1978**, qu'a été adoptée la première norme de droit français sur la protection des données (sous la présidence de M. Giscard d'Estaing, européen fervent). Le législateur de 1978 avait alors perçu la nécessité

² Jean-Marc Sauvé, op. cit.

de réguler le traitement des données personnelles, en particulier par les organes de l'Etat et les personnes publiques en général, qui étaient alors perçues comme la source principale de danger. En effet, dans les années 1970, était apparu un risque d'un fichage de l'ensemble de la population française, avec un projet SAFARI qui prévoyait l'identification de chaque citoyen sous un fichier unique... Et parmi les autorités qui suscitaient la méfiance du législateur, il y avait non seulement l'administration, mais aussi le juge, puisque l'article 2 de la loi de 1978, dans sa version initiale, disait : « *aucune décision de justice impliquant une appréciation sur un comportement humain ne peut avoir pour fondement un traitement automatisé d'information donnant une définition du profil ou de la personnalité de l'intéressé...* »

La grande nouveauté de la loi du 6 janvier 1978 a été la création d'une « **COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES**, qu'on appelle en français, par abréviation, **CNIL** (*KNIL*), dotée de véritables pouvoirs de décision, la loi attribuant notamment à la commission un pouvoir normatif (*pouvoir réglementaire*).

La loi de 1978 a défini la CNIL, comme une **AUTORITE ADMINISTRATIVE INDEPENDANTE** (littéralement *unabhängige Verwaltungsbehörde*)³. Il y a là un concept d'origine américaine⁴ (*authority*) ou scandinave. Mais dans les pays

³ cf rapport Jean-Marie Ponthier professeur à l'Université d'Aix Marseille III

⁴ Cf the *Interstate commerce commission* créée au XIX ème siècle pour contrôler les entreprises ferroviaires de transport. Cf concept d'agencies

anglo-saxons, on est réticent à qualifier ces organes comme étant « administratifs »⁵.

La CNIL est donc une autorité « administrative », oui, mais le législateur s'est efforcé de lui donner une composition pour lui garantir son indépendance :

17 membres en 1978, 18 aujourd'hui (je donne la composition actuelle, mais elle a peu changé depuis 1978) : 2 députés élus par l'Assemblée nationale, deux sénateurs, **2 membres du Conseil d'Etat** élus par l'AG du CE, 2 membres de la Cour de cassation élus par AG de la cour, 2 membres de la Cour des comptes, deux personnalités qualifiées en informatique nommés par décret sur proposition du président de l'AN et du Sénat, 3 personnalités qualifiées pour leur connaissance du numérique et des questions touchant aux libertés individuelles nommées par décret, et des questions touchant aux libertés individuelles, désignées respectivement par le président de l'Assemblée nationale et le président du Sénat, et enfin le président, nommé par le président de la République.

C'est donc une composition mixte, avec des parlementaires, des juges des 2 cours suprêmes administratives et judiciaires, des membres à qualité nommés par le gouvernement. Le président de la commission est nommé par le président de la

⁵ Ainsi, les Quangos en Grande Bretagne sont des *quasi autonomous non governmental organizations*. Il appartiendra à nos collègues allemands de dire si les *Selbständige Bundesoberbehörden*, les *Zentralstelle* les *Anstalten des öffentlichen Rechts* par exemple le *Bundesanstalt für Finanzdienstleistungsaufsicht*) correspondent à ce que l'on appelle en droit français des autorités administratives indépendantes. Quant à l'Italie, les *autorità amministrative indipendenti* apparues depuis les années 70 seraient, paraît-il, inspirées plus ou moins de l'expérience française tout en recouvrant des réalités très diverses pouvoir neutre ou pouvoir de garantie selon la doctrine italienne, forse l'*Autorità per le garanzie delle comunicazioni* potrebbe essere paragonata alla CNIL francese.

République. Le mandat des membres est de 5 ans. Cette composition est censée assurer son indépendance, mais des critiques sont émises à ce sujet⁶.

Le fait que la CNIL (commission nationale Informatique et Libertés) ait été définie par la loi de 1978 comme une *autorité administrative indépendante* a une conséquence importante pour notre thème : Les diverses décisions que cet organisme prend vont être soumises au contrôle du juge administratif. Et dès les années qui suivent l'adoption de la loi de 1978, on trouve des décisions du Conseil d'Etat, qui annulent des décisions de la CNIL.⁷

Bien entendu, la protection des données dans les années 1970 n'était pas une préoccupation exclusivement française. Elles se sont manifestées dans tous les pays européens, (pour me limiter au vieux continent)⁸.

⁶ Des critiques sont adressées à **la CNIL** : CNIL remise en cause locaux occupés en 2007 un collectif dénonce sa pseudo indépendance depuis juillet 2004 la loi a décidé que les services de police n'auraient même pas à s'asseoir sur les avis de la CNIL pour créer de nouveaux fichiers. En février 2013 Gilles Babinet, digital champion attaque vivement l'autorité dans un magazine l'usine nouvelle la CNIL pénaliserait le développement du numérique en France ; l'autorité serait trop acboutée sur la défense des libertés individuelles, administration en décalage avec les aspirations de la société civile en matière d'innovation.

⁷ Voir par exemple Conseil d'Etat 12 mars 1982 n° 25173 Requête de la Confédération générale du travail tendant à l'annulation de la délibération du 18 mars 1980 de la Commission nationale de l'informatique et des libertés portant adoption de la norme simplifiée concernant les traitements automatisés d'informations nominatives relatifs à la paie et à la gestion des personnels des personnes physiques et morales autres que celles gérant un service public ;

⁸ Ces préoccupations se manifestent en dehors de l'Europe, en Inde par exemple, où la cour suprême a décidé le 29 septembre dernier, de restreindre le partage des données relatives à la carte d'identité du pays par rapport aux entreprises privées, l'Inde étant dotée de la plus grande base de données biométriques du monde

L'Allemagne semble avoir été, avec la loi fédérale de 1977 portant protection contre l'emploi abusif des données d'identification personnelle, le premier pays à adopter un texte sur la protection des données personnelles. L'Italie a suivi le mouvement à son tour, notamment lorsqu'a été adoptée la loi du 31 décembre 1996⁹ (*prima del 30 giugno 2003 e del DL sul codice in materia di protezione dei dati personali*).

Avec l'apparition et le développement d'Internet, est apparue la volonté au niveau de l'Union européenne, de réguler la matière.

Ainsi, a été adoptée, la **directive 95/46/CE du 24 octobre 1995 sur la protection des données personnelles** (Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr) (Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati).

En France, cette directive a été transposée relativement tard, par une loi du 6 août 2004, relative à la protection des personnes physiques.

Toutefois, le risque d'un manque d'harmonie entre les différents pays européens a imposé en 2016, l'adoption, non plus d'une directive, qui se borne à fixer des objectifs aux Etats membres, mais d'un **règlement européen**, texte qui s'applique

⁹ Qui concernait les personnes physiques et les personnes morales.

directement et totalement dans les Etats membres. Il s'agit du règlement qui est l'objet de notre étude :

- REGLEMENT EUROPEEN 2016-679 DU 27 AVRIL 2016, sur la protection des *personnes physiques* a l'égard du traitement des données à caractère personnel et à la libre circulation de ces données¹⁰, abrogeant la directive 95/46/ce.

Ce règlement est appelé en français, par abréviation, RGPD et on l'appellera ainsi au cours de cette étude.

- VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

- REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

II ENTREE EN VIGUEUR DU REGLEMENT EUROPEEN

¹⁰ Après la directive 95/46/CE

Et c'est bien l'entrée en vigueur de ce règlement, le RGPD donc, qui pose problème pour cette étude. D'abord, parce que c'est un texte long et touffu, (rien que dans l'introduction, il y a 173 considérants), complexe et technique, particulièrement difficile à aborder par les entreprises et les administrations, pour ne rien dire du juge !

Ainsi, dans un article du 18 octobre 2016, le journal La Tribune écrivait que « *96% des entreprises des trois principales économies européennes [France, Allemagne, Royaume-Uni] ne comprennent pas encore clairement le Règlement général de protection des données (RGPD) (...) Selon une étude publiée ce mardi par la société de sécurité informatique Symantec, 92% des dirigeants et décideurs français s'inquiètent de ne pas être en conformité au moment de l'entrée en vigueur de la RGPD* » !

Mais c'est surtout les conditions de l'entrée en vigueur d'un règlement, adopté en 1995 après 4 années d'âpres négociations, qui est source de difficultés pour notre sujet.

Première remarque, l'article 99 du règlement (Entrée en vigueur et application) dit que : « *1. Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au Journal officiel de l'Union européenne. / 2. **Il est applicable à partir du 25 mai 2018*** ». 25 mai 2018, cela veut dire que si nous examinons les questions posées par l'application de ce règlement devant le juge administratif, cela veut dire que beaucoup de ces questions restent ouvertes ou relèvent même de la prospective juridique, comme nous le verrons.

Ensuite, comme on le sait, contrairement à une *directive*, un *règlement* adopté par le Conseil et le Parlement européens, est **d'application directe** et s'impose en principe aux États Membres à compter du 25 mai 2018, et il ne devrait pas être nécessaire, en théorie, de le transposer dans les législations nationales.

En fait, le RGPD contient deux catégories de dispositions : certaines se substituent complètement aux règles des États membres en accordant directement des droits aux personnes dont les droits ont été violés par un système de traitement des données ¹¹. Mais sur d'autres points, le règlement est un peu comme une directive, il laisse aux États membres la possibilité de conférer des droits aux personnes ou d'imposer des obligations ou de prévoir des procédures dans le cadre national, en complétant ainsi le RGPD. C'est ce que l'on appelle les « **marges de manœuvre nationales** » laissées aux États membres.

Il en résulte qu'en France, la *loi Informatique et libertés* de 1978 reste en vigueur et vient compléter le RGPD :

Il s'agit par exemple du traitement des données de santé ou des données d'infraction, de la fixation à 15 ans du seuil d'âge du consentement des mineurs aux services en ligne, des dispositions relatives à la mort numérique, etc. En outre, la loi nationale reste pleinement applicable pour tous les fichiers « répressifs », qu'il s'agisse de la sphère pénale ou du domaine du renseignement et de la sûreté de l'État. De nombreuses dispositions spéciales sont prévues en ces matières.

¹¹ droits des personnes, bases légales des traitements, mesures de sécurité à mettre en œuvre, transferts, etc.

Cette situation quelque peu compliquée fait que une loi nouvelle a été adoptée par le parlement français pour modifier la loi de 1978 et la mettre, en principe, en conformité avec le règlement européen RGPD : Il s'agit de la **loi n° 2018-493 du 20 juin 2018**, promulguée le 21 juin 2018, dite **CNIL 3**, qui vient donc d'une part rapprocher de la loi française de la lettre du RGPD et d'autre part, exercer certaines « marges de manœuvre nationales ».

Toutefois, la complexité résultant de la combinaison du règlement européen et de la loi nationale n'est pas, loin de là, complètement réglée, tant et si bien qu'une ordonnance du gouvernement (expliquer ce qu'est une ordonnance de l'article 38 de la constitution française) de réécriture complète de la loi de 1978 (Informatique et Libertés) est prévue dans un délai de six mois, notamment afin de résoudre ces difficultés de lisibilité de ce cadre juridique composite !

Nous sommes ainsi, en France, dans une situation où, en cas de conflit entre la loi nationale et le règlement européen, le juge appliquera normalement la loi interne, qui joue ainsi le rôle d'une « loi-écran » entre le droit européen et la réglementation française, sauf à ce que les requérants ou les requérantes soulèvent la contrariété de la loi par rapport au règlement européen, le RGPD, ce qui déclenchera la procédure de contrôle de la conformité de la loi en cause par

rapport au règlement, selon la procédure française dite de contrôle de conventionalité initié par la jurisprudence du Conseil d'Etat *Nicolo*.¹²

De plus, le droit national a dû également être complété par un nouveau décret d'application de la loi Informatique et Libertés pour achever la mise en conformité du droit national au cadre juridique européen. Ce décret est intervenu le 1^{er} août 2018.¹³

Enfin, il y a eu une décision du Conseil constitutionnel français n° 2018-765 DC du 12 juin 2018. Les sénateurs requérants ont déféré au Conseil constitutionnel la loi du 20 juin 2018, en dénonçant son inintelligibilité et en soutenant que le texte déféré méconnaît l'objectif de valeur constitutionnelle d'accessibilité et d'intelligibilité de la loi compte tenu des divergences résultant de l'articulation entre les dispositions de la loi du 6 janvier 1978, telle que modifiée, et du règlement du 27 avril 2016 mentionnés ci-dessus. Selon eux, cette absence de

¹² Article 5-1 de la loi informatique et libertés modifiée dit que : Les règles nationales prises sur le fondement des dispositions du règlement s'appliquent dès lors que la personne concernée réside en France, y compris lorsque le responsable de traitement n'est pas établi en France. Toutefois, lorsqu'est en cause un des traitements mentionnés au 2 de l'article 85 du même règlement, les règles nationales mentionnées au premier alinéa du présent article sont celles dont relève le responsable de traitement, lorsqu'il est établi dans l'Union européenne.

¹³ Décret n° 2018-687 du 1er août 2018 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles. Il permet de fixer plus précisément les procédures de traitement par la CNIL des différents dossiers dont elle a la charge et de préciser certaines dispositions de la loi.

lisibilité était de nature à « induire gravement en erreur » les citoyens quant à la portée de leurs droits et obligations en matière de protection des données personnelles. Le conseil constitutionnel a écarté cet argument.

« En outre, le RGPD est accompagné d'une directive n°2016/680 du Parlement Européen et du Conseil, adoptée le même jour que le RGPD mais destinée aux autorités administratives, et relative à « la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données. »¹⁴.

Le juge administratif français va avoir un travail considérable pour interpréter ces textes ! Remarquons qu'en cas de conflit entre la norme européenne et la loi interne française, les requérants et les requérantes pourront toujours soulever, devant le juge, l'*inconventionnalité* de la loi française par rapport au règlement européen¹⁵, c'est-à-dire le fait qu'une loi française est contraire à un texte de niveau européen.

III LE CONTENU DU RGPD : SES INCIDENCES SUR LE DROIT ADMINISTRATIF ET LA JURIDICTION ADMINISTRATIVE FRANÇAISE

¹⁴ Voir <https://www.village-justice.com/.../RGPD-Reglement-General-sur-Protection-des-Donn...> 14 déc. 2016 - RGPD : le Règlement Général sur la Protection des Données qui bouleverse la loi ... Par Bernard Rineau, Avocat, et Julien Marcel, Juriste. ..

¹⁵ Par l'arrêt *Nicolo* du 20 octobre 1989, le Conseil d'État a accepté de contrôler la compatibilité d'une loi avec les stipulations d'un traité, même lorsque la loi est postérieure à l'acte international en cause, en application de l'article 55 de la Constitution, abandonnant ainsi la théorie de la loi écran.

Elles sont multiples et il ne saurait être question ici de les analyser toutes.

- Incidences sur la CNIL (commission nationale informatique et libertés)

Le RGPD s'est efforcé de redéfinir le rôle des autorités de protection des données des pays membres. Dans son article 4, au paragraphe 21, le RGPD parle en effet d'une «autorité de contrôle», une autorité publique indépendante instituée par un État membre, qui est une autorité de contrôle concernée par le traitement de données à caractère personnel.

Tout naturellement, la loi française du 20 juin 2018, modifiant la loi du 6 janvier 1978, désigne **la CNIL comme l'autorité de contrôle nationale au sens et pour l'application du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016.**

L'adoption du RGPD entraîne une redéfinition et même un élargissement des pouvoirs de la CNIL (commission nationale de l'informatique et des libertés) par la loi du 20 juin 2018. Sur ce point, je me limiterai à mettre en évidence deux aspects de cette évolution des pouvoirs de la CNIL :

1° alors que le système juridique français privilégiait le contrôle *a priori* des traitements de données personnelles, le choix européen va au contraire dans le sens d'un contrôle *a posteriori* pour favoriser une libéralisation de l'espace communautaire. Ainsi et à part les cas où le droit des États membres peut maintenir des autorisations pour certaines catégories de données ou de traitements

(par exemple en matière de santé), la plupart des obligations déclaratives et des autorisations préalables que délivraient la CNIL sont supprimées.

Toutefois demeurent soumis à autorisation par arrêté du ou des ministres compétents, *pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés*, certains **traitements de données à caractère personnel mis en oeuvre pour le compte de l'Etat**, notamment ¹⁶:

1° Qui intéressent **la sûreté de l'Etat, la défense ou la sécurité publique** ;

2° Ou qui ont pour objet **les infractions pénales** ;

Certains traitements portant sur des données à **caractère personnel qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques etc...** sont autorisés par décret en Conseil d'Etat pris après avis motivé et publié de la commission ;

2° Le RGPD et la loi donnent aux autorités de protection et donc en France à la CNIL, des pouvoirs de sanction et notamment celui de prononcer des **amendes administratives très importantes**. L'article 83 du RGPD prévoit de façon assez précise les conditions relatives à ces amendes. En cas de violation du règlement, ces amendes seraient susceptibles désormais, selon le règlement, d'atteindre, selon la catégorie du manquement, 10 à 20 millions d'euros ou, dans le cas d'une entreprise, 2% à 4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu. Les États membres peuvent même prévoir ou non dans leur législation des amendes à infliger aux autorités et organismes publics. Mais la

¹⁶ Voir Article 26 de la loi de 1978, modifié par la loi du 20 juin 1978.

détermination de ces sanctions est laissée par le règlement à l'appréciation des Etats (c'est un exemple de « marge de manœuvre nationale"). Par exemple, la CNIL a infligé en juin 2018 une amende record de 250.000 euros à la chaîne de magasins d'optique *Optical Center*, pour une atteinte à la sécurité des données de ses clients. C'est la première fois que la CNIL (Commission nationale de l'informatique et des libertés) impose une amende aussi forte, a-t-on appris auprès de l'autorité ¹⁷.

Accroissement des compétences de la CNIL, pouvoir d'infliger des sanctions administratives, tout cela peut être la source d'un accroissement du contentieux devant le Conseil d'Etat.

- Incidences sur le juge administratif français:

a) sur le juge administratif en général :

Dans le cadre des « marges de manœuvre nationales », la loi du 20 juin 2018 précise, en son article 10, « *qu'aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de la personnalité de cette personne* ».

¹⁷ SOURCE : site Le Figaro

Dans cette optique, l'anonymisation des décisions de justice contenues dans les banques de données devant la juridiction administrative française semble une bonne chose.

Il faut noter que l'article 10 de la loi du 6 janvier 1978, modifiée par la loi du 20 juin 2018, a par ailleurs prévu les cas dans lesquels, par exception, une décision administrative individuelle peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel, dès lors que l'algorithme de traitement utilisé ne porte pas sur des données sensibles, que des recours administratifs sont possibles et qu'une information est délivrée sur l'usage de l'algorithme.

Le Conseil constitutionnel a examiné la constitutionnalité de cette disposition. Les requérants estiment qu'en autorisant l'administration à prendre des décisions individuelles sur le seul fondement d'un algorithme, celle-ci serait conduite à renoncer à l'exercice de son pouvoir d'appréciation des situations individuelles. Mais le conseil constitutionnel a écarté cette argumentation en jugeant que la loi française a défini des garanties appropriées pour la sauvegarde des droits et libertés des personnes soumises aux décisions administratives individuelles prises sur le fondement exclusif d'un algorithme.

b) sur le Conseil d'Etat français en particulier :

- Dès lors qu'en matière de protection des données, l'autorité administrative indépendante nationale (elle siège à Paris) qu'est la CNIL joue un rôle essentiel, le juge administratif compétent à l'égard des décisions et actions de celle-ci est le CONSEIL D'ETAT, juridiction administrative suprême, ou pour reprendre l'expression usitée, juge ultime de l'administration. En effet, la loi française, et plus particulièrement le CODE DE JUSTICE ADMINISTRATIVE, dit en son

article R311-1 que le Conseil d'Etat est compétent pour connaître en premier et dernier ressort :

« 4° *Des recours dirigés contre les décisions prises par les organes des autorités suivantes, au titre de leur mission de contrôle ou de régulation : la **Commission nationale de l'informatique et des libertés*** » (CNIL).

On a donc, jusqu'à présent, en France, du fait de l'activité de la CNIL, un contentieux très centralisé devant le Conseil d'Etat.

Quelles sont les conséquences de l'entrée en vigueur du RGPD sur les voies de recours devant la juridiction administrative ?

- Dans son chapitre VIII, en ses articles 77 à 82, le RGPD contient des dispositions assez précises sur les voies de recours et la responsabilité. Pour me limiter à celles qui sont susceptibles d'intéresser directement le Conseil d'Etat, je citerai :

Les articles 78 et 79 du RGPD prévoient le droit à un recours juridictionnel *effectif* contre une autorité de contrôle pour toute personne physique et morale... ou contre un responsable du traitement ou un sous-traitant. On peut estimer que le contrôle exercé par le Conseil d'Etat sur les décisions de la CNIL répond très largement à ces exigences. **Notamment, les décisions prises par la CNIL peuvent faire l'objet des procédures de référé, référé suspension et référé liberté, prévues aux articles L 521-1 et L 521-2 du code de justice administrative.**

Mais précisément, l'entrée en vigueur du RGPD a eu pour conséquence l'adoption, dans la loi de 1978, modifiée par la récente loi du 20 juin 2018, d'une disposition (article 46 IV de la loi), selon laquelle « *le président de la CNIL peut demander, par la voie du référé, à la juridiction judiciaire ou administrative, d'ordonner, le cas échéant sous astreinte, toute mesure nécessaire à la sauvegarde de ces droits et libertés* ».

En matière administrative, cela s'applique directement **au référé-liberté visé par l'article L 521-2 du code de justice administrative**. Je rappelle qu'en droit français, le référé liberté est un **recours d'extrême urgence** (le juge doit statuer dans les 48 heures) **tendant à ce que le juge des référés ordonne toutes mesures nécessaires à la sauvegarde d'une liberté fondamentale à laquelle l'administration aurait porté une atteinte grave et manifestement illégale**. Eh bien, pour appliquer le RGPD et la loi du 20 juin 2018, il a été jugé nécessaire d'introduire, de façon très récente, une modification du code de justice administrative ¹⁸, avec l'adoption d'une disposition expresse visant la procédure applicable lorsque le président de la CNIL saisit le juge administratif des référés dans le cadre d'un référé liberté. Il s'agit de l'article R555-1 du code de justice administrative ¹⁹ qui est venu en quelque sorte préciser les conditions

¹⁸ Décret n°2018-687 du 1er août 2018 - art. 30

¹⁹ « Lorsque le juge administratif est saisi par le président de la Commission nationale de l'informatique et des libertés, sur le fondement du IV de l'article 46 de la loi n° 78-17 du 6 janvier 1978 relative à

d'application du référé-liberté en cas d'atteinte grave et immédiate aux libertés du fait de la violation des dispositions du RGPD par une personne publique, par exemple l'Etat ou une autorité locale, telle qu'une commune. Sans rentrer dans le détail d'une analyse juridique complexe, je vois pour la jurisprudence future du Conseil d'Etat une belle question à trancher du fait de la combinaison de la loi du 2 janvier 1978, dans sa version modifiée du fait de l'introduction du RGPE, avec l'article L 521-2 du code de justice administrative : Lorsque le Conseil d'Etat est saisi d'un référé liberté par le président de la CNIL, est ce que c'est la condition d'une urgence simple qui s'applique ou la condition d'extrême urgence telle qu'elle est prévue par la procédure du référé-liberté ?

Ajoutons qu'une autre disposition du code de justice administrative, mais qui n'entrera en application que le 1^{er} janvier 2019, introduit des mesures semblables en ce qui concerne un autre référé possible devant la juridiction administrative, dit référé mesures utiles (L.521-3 du code de justice administrative). Toute personne pourra demander au juge administratif des référés de prononcer « *toutes mesures utiles de nature à éviter toute dissimulation ou toute disparition de données à caractère personnel par l'Etat, une collectivité territoriale ou toute autre personne publique* ».

l'informatique, aux fichiers et aux libertés, d'une demande en référé concernant la mise en oeuvre d'un traitement ou l'exploitation de données à caractère personnel par l'Etat, une collectivité territoriale, toute autre personne publique ainsi que toute personne privée chargée d'une mission de service public, il est statué suivant la procédure de référé instituée par les dispositions de l'article L. 521-2 ».

- L'article 80 du RGPD, et c'est le cœur de notre sujet, **confère directement à la personne dont les droits ont été violés le droit de « *mandater un organisme, une organisation ou une association à but non lucratif, ..., dont les objectifs statutaires sont d'intérêt public et est actif dans le domaine de la protection des droits et libertés des personnes concernées dans le cadre de la protection des données à caractère personnel les concernant, pour introduire une réclamation en son nom, exerce en son nom les droits visés aux articles 77, 78 et 79 et exerce en son nom le droit d'obtenir réparation visé à l'article 82 lorsque le droit d'un État membre le prévoit* »**. Observons que qu'il s'agit là d'un droit directement conféré à la personne, et qui est donc directement applicable en droit interne français. Pour la France, il concerne spécialement les recours en responsabilité, ou les recours de pleine juridiction. Rappelons que la juridiction administrative française ne juge pas les seuls recours en annulation d'une décision administrative, mais qu'une part très importante de son activité est consacrée à l'examen des recours en responsabilité contre les personnes publiques.

L'article 80 du RGPD consacre l'abandon d'un principe fondamental qu'on appliquait traditionnellement devant la juridiction administrative française, qui disait : « *Nul ne plaide par procureur* » « *nemo petit ab accusatore* ». La jurisprudence traditionnelle qui interdit à un groupement, par exemple un syndicat ou une association, d'introduire directement un recours au lieu et place de la personne lésée n'est ainsi, dans la matière de la protection des données à caractère

personnel, plus valable, du moins pour les recours tendant à engager la responsabilité des personnes publiques, Etat, communes, etc...

Les commentateurs estiment qu'ainsi, le **RGPD prévoit une action de groupe**.

On vise ainsi une procédure de poursuite collective qui permet par exemple à des consommateurs, victimes d'un même préjudice de la part d'un professionnel, de se regrouper et d'agir en justice. Les plaignants peuvent par exemple se défendre avec un seul dossier et un seul avocat.

En fait, l'action de groupe a été introduite en France dès 2014, dans le domaine de la consommation²⁰, et elle a fait l'objet d'une loi n° 2016-1547 du 18 novembre 2016, dite de modernisation de la justice du XXI^e siècle qui a créé un cadre légal commun aux actions de groupe en matière judiciaire et administrative et qui vient modifier profondément, voire bouleverser, les règles traditionnelles notamment en matière d'intérêt à agir.

Cette loi de 2016 a entraîné une modification du code de justice administrative, adoptée après l'édiction du RGPD, mais avant son entrée en vigueur, ce qui fait que le code de justice administrative définit aujourd'hui avec un grand luxe de détails la portée des actions de groupe, en visant en particulier les actions ouvertes sur le fondement de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (article 43 ter).

²⁰ loi n° 2014-344 du 17 mars 2014 relative à la consommation,

L'action de groupe prend deux formes : elle peut être exercée en vue soit de l'engagement de la responsabilité de la personne ayant causé le dommage afin d'obtenir la réparation des préjudices subis, soit de la cessation du manquement mentionné au premier alinéa, soit les deux en même temps. Selon le code de justice administrative modifié, **lorsque l'action de groupe tend à la cessation d'un manquement, le juge, s'il constate l'existence de ce manquement, dispose d'un pouvoir d'injonction au défendeur de cesser ou de faire cesser ledit manquement et de prendre, dans un délai qu'il fixe, toutes les mesures utiles à cette fin.**

Cependant, pour tenir compte du RGPD, la loi du 18 novembre 2016 a dû être modifiée par la loi du 20 juin 2018, avec l'objectif (article 43 ter) en particulier de préciser les conditions d'application du code de justice administrative relative aux actions de groupe en matière de manquement par une personne publique aux dispositions du RGPD.

L'idée principale à retenir est que l'action de groupe est limitée aux :

- 1° Les associations régulièrement déclarées depuis cinq ans au moins ayant pour objet statutaire la protection de la vie privée et la protection des données à caractère personnel ;
- 2° Les associations de défense des consommateurs représentatives au niveau national et agréées,

3° Les organisations syndicales de salariés ou de fonctionnaires représentatives ou les syndicats représentatifs de magistrats de l'ordre judiciaire, lorsque le traitement affecte les intérêts des personnes que les statuts de ces organisations les chargent de défendre.

Précisons, pour en terminer avec ces actions de groupe concernant la violation des règles relatives à la protection des données, qu'elles peuvent donner au lieu à des actions devant l'ensemble des juridictions administratives, et non plus devant le seul Conseil d'Etat, compétent, comme il a été dit ci-dessus, pour juger des recours dirigés contre les décisions prises par les organes des autorités suivantes, au titre de leur mission de contrôle ou de régulation : la **Commission nationale de l'informatique et des libertés** » (CNIL).

- L'article 81 du RGPD²¹ introduit une sorte de sursis à statuer pour les juridictions européennes au cas où une action contre le même responsable du traitement ou le même sous-traitant est pendante devant la juridiction d'un autre Etat membre, toute juridiction compétente autre que la première juridiction saisie en premier lieu peut « suspendre son action », c'est-à-dire surseoir à statuer. Il y a là, selon le règlement, une possibilité et non une obligation.

²¹ Article 81 du RGPD : « Lorsqu'une juridiction compétente d'un État membre est informée qu'une action concernant le même objet a été intentée à l'égard d'un traitement effectué par le même responsable du traitement ou le même sous-traitant et est pendante devant une juridiction d'un autre État membre, elle contacte cette juridiction dans l'autre État membre pour confirmer l'existence d'une telle action. / **Lorsqu'une action concernant le même objet a été intentée à l'égard d'un traitement effectué par le même responsable du traitement ou le même sous-traitant et est pendante devant une juridiction d'un autre État membre, toute juridiction compétente autre que la juridiction saisie en premier lieu peut suspendre son action.** / Lorsque cette action est pendante devant des juridictions du premier degré, toute juridiction autre que la juridiction saisie en premier lieu peut également se dessaisir, à la demande de l'une des parties, à condition que la juridiction saisie en premier lieu soit compétente pour connaître des actions en question et que le droit applicable permette leur jonction.

Par ailleurs, le RGPD contient, en son article 82, des dispositions spécifiques aux recours en responsabilité : Il confère à toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi. A vrai dire, et sous réserve de règles relatives à la solidarité et à la subrogation entre plusieurs responsables du traitement ou sous-traitants en cas de dommage causé par un traitement, les règles fondamentales en vigueur dans le droit interne français ne paraissent pas substantiellement modifiées, notamment au niveau des règles d'imputabilité.

IV JURISPRUDENCE

Je n'ai pas trouvé de jurisprudence récente quant aux questions soulevées par l'entrée en vigueur du RGPD et de la loi du 20 juin 2018, à part la décision du conseil constitutionnel n° 2018-765 DC du 12 juin 2018, évoquée plus haut.

Je me limiterai à citer les quelques décisions suivantes :

- **Conseil constitutionnel n°2016-536 QPC du 19 février 2016, *Ligue des droits de l'Homme***, cons. 11 et 14 :A cet égard, si le contexte de l'état d'urgence justifie l'exercice d'un contrôle juridictionnel *a posteriori* sur des mesures de perquisition administrative, il ne saurait pour autant permettre la saisie de données informatiques, ni leur exploitation, sans l'autorisation préalable d'un juge :

- 9 mars 2018 : la CNIL, en tant que personnalité chargée de s'assurer du contrôle de la liste noire, saisit **le tribunal administratif de Paris** pour contester la

décision du ministre de l'intérieur selon laquelle 4 publications d'Indymedia, qui revendiquaient des incendies commis dans plusieurs villes de France seraient des incitations au terrorisme. (Source site Nextimpact).

- **Conseil d'Etat** : 3 juin 2013 n° 328634 : le Conseil a décliné sa compétence en premier et dernier ressort pour statuer sur un recours formé contre une décision de la CNIL refusant l'accès aux données d'un fichier à un demandeur par le ministre de l'intérieur.

- **Conseil d'Etat** 7 février 2014 : sur une sanction 150 000 euros prononcée par la CNIL contre Google pour manquement aux règles de protection des données. Pas d'urgence à statuer.

- **Conseil d'Etat Ordonnance** du 19 février 2008 : premier référé suspension à l'encontre d'une décision de sanction de la CNIL. Le juge des référés rejette la requête d'une demande de suspension de l'exécution d'une décision de la CNIL enjoignant de cesser la mise en œuvre d'un traitement. **Le Conseil d'Etat juge que la CNIL est une juridiction au sens de l'article 6-1 de la Convention Européenne des Droits de l'Homme.** La CNIL doit donc agir comme un tribunal indépendant et impartial et ses audiences doivent être publiques.

- **CONCLUSION**

Sujet qui combine la complexité de l'informatique et du droit !

On voit que le juge administratif français, et la remarque est sans doute identique pour les juges administratifs allemands et italiens, se trouve au cœur de questions essentielles pour les Etats et la société en Europe. Le juge administratif entend

maintenir son rôle de gardien des libertés, combiné avec celui d'appliquer le droit européen, dans le cadre d'un système de dualité d'ordres de juridiction. L'enchevêtrement des textes européens et nationaux en matière de régulation de la circulation de l'information par Internet et d'accès aux banques de données rend cependant sa tâche de plus en plus difficile. Aujourd'hui, alors que certains observateurs estiment que le RGPD est déjà dépassé sous certains aspects, il faut augurer que les juges administratifs de nos trois pays sauront s'adapter à cette évolution permanente, pour ne pas dire cette mutation.