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

Aujourd'hui, l'essor extraordinaire d'Internet et des réseaux sociaux permet une circulation mondiale des informations, qui sont devenues la matière première de l'activité des géants du Web, ces fameux GAFA, (=GOOGLE, Apple, Facebook et Amazone). Cette circulation comporte un risque considérable de violation des données personnelles de chacune et de chacun, de sa *privacy* [1]. D'où l'idée de tenter de réguler ce phénomène par des instruments juridiques au sein des Etats ou au niveau européen[2]. La problématique de la régulation européenne s'inscrit dans un cadre libéral sous la forme d'une dialectique : D'une part, il faut essayer de faciliter la circulation de l'information par les réseaux, sans y mettre des entraves excessives. D'autre part il est essentiel de préserver les droits et libertés des citoyens, « *dont les données peuvent être erronées, collectées et conservées de manière injustifiée ou disproportionnée … ou susceptibles de révéler, sur chaque personne, des habitudes, des préférences ou des opinions*[3] » [4]. C'est sur cette dialectique qu'est fondé le Règlement européen qui est entré en vigueur le 25 mai 2018 : assurer la libre circulation de l'information tout en préservant les droits des citoyens, au moyen de l'existence d'autorités de contrôle et d'un contrôle juridictionnel *effectif.* Ainsi est consacrée l'importance du rôle du juge en général et du juge administratif en particulier, lequel entend maintenir en France toute sa place en tant que protecteur des droits et des libertés.

En France, c'est avec la loi du 6 janvier 1978 qu'a été adoptée la première norme de droit sur la protection des données (sous la présidence de M. Giscard d'Estaing, européen fervent s'il en est). A cette époque, la nécessité de réguler le traitement des données personnelles visait essentiellement à protéger les citoyennes et les citoyens contre l'Etat et les personnes publiques, alors perçues comme la source principale de danger. Parmi les autorités qui suscitaient la méfiance du législateur, il y avait même le juge !

---

[1] En 2014, plus d'un milliard de sites en ligne, 3 milliards d'internautes.

[2] Aux Etat Unis, il n'y a pas, pour l'instant de législation générale au niveau fédéral sur le traitement des données

[3] Jean-Marc Sauvé, op. cit.

[4] Sous cet aspect, la CNIL vient de rappeler ces derniers jours (janvier 2019) qu'elle a enregistré plus de 1 200 violations de données personnelles.

Bien entendu, la protection des données personnelles n'est pas une préoccupation exclusivement française[5]. L'Allemagne semble avoir été, avec une loi fédérale de 1977, le premier pays européen à adopter un texte sur la protection des données personnelles. Pour sa part, l'Italie a adopté une loi en la matière le 31 décembre 1996[6].

Au niveau européen ont d'abord été adoptées plusieurs directives : par exemple,[7] lesquelles ont été transposées dans la législation nationale française sous la forme de modifications apportées successivement à la loi du 6 janvier 1978.

Toutefois, le risque d'un manque d'harmonie entre les différents Etats a imposé en 2016 l'adoption, non plus d'une directive, dont on rappellera qu'il s'agit d'un texte qui se limite à fixer des objectifs, mais d'un **règlement européen** qui s'applique, à la différence d'une directive, directement et totalement dans les Etats membres. Il s'agit du règlement qui est l'objet de notre étude, soit **le REGLEMENT EUROPEEN 2016-679 DU 27 AVRIL 2016, sur la protection des *personnes physiques* à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[8], abrogeant la directive 95/46/ce[9] ou**

---

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

[6] Qui concernait les personnes physiques et les personnes morales.

[7] Cf par ex 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).

[8] Après la directive 95/46/CE

[9] Die 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).

Il 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,

RGPD, [10] adopté par le Parlement européen et le Conseil le 27 avril 2016 et publié le 4 mai 2016 au *Journal officiel de l'Union européenne*.

La plupart des commentateurs estime que ce règlement pose une foule de questions qu'il est impossible de trancher toutes ici. Mon propos se limitera à essayer de situer la place du juge administratif dans l'application du RGPD. Je donnerai quelques aperçus sur l'Allemagne et l'Italie, car la présente intervention est la reprise d'une autre intervention que j'ai effectuée lors d'un colloque organisé par **l'Association des Juges Administratifs Français, Italiens et Allemands (AJAFIA)** en octobre dernier à Saarbruck, en Allemagne.

PLAN DE L'INTERVENTION

I LE JUGE FACE AU RGPD : QUELS TEXTES APPLICABLES

II LE JUGE DANS LE CADRE DU RGPD

III APERÇU DE JURISPRUDENCE

I LE JUGE FACE AU RGPD : QUELS TEXTES APPLICABLES ?

L'article 99 du règlement européen introduit une différence subtile entre entrée en vigueur et application. L'article 99 dit en effet que : « 1. *Le présent règlement* ***entre en vigueur*** *le vingtième jour suivant celui de sa publication au Journal officiel de l'Union européenne* », comme c'est le cas normalement pour les règlements européens. Mais le second alinéa de l'article 99 poursuit : « 2. ***Il est applicable à partir du 25 mai 2018*** », soit deux ans après son adoption, [11] dans tous les Etats membres de l'UE.

---

nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

[10] Le même jour était adoptée une DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 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, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

[11] L'application dans le temps des règlements de l'Union européenne n'est en effet pas homogène. Certains précisent leur date d'entrée en vigueur, sans donner d'indication sur la date d'application. D'autres précisent leur date d'application sans préciser leur date d'entrée en vigueur. D'autres encore contiennent des dispositions transitoires. Inutile de dire combien ces

Des difficultés pourraient se poser en fonction de cette différenciation entre *l'entrée en vigueur* et l'*application*. Certains juristes en déduisent par exemple que dès la date *d'entrée en vigueur*, soit à la date du 24 mai 2016, les Etats membres ne pouvaient prendre de mesures contraires au RGPD. En tout cas, depuis sa date *d'entrée en application*, le 25 mai 2018, le règlement est opposable aux particuliers et aux entreprises. On ne peut qu'observer que le 25 mai 2018 est, pour une réflexion entreprise à la date du 23 janvier 2019, une date encore bien récente.

Ensuite, comme il a déjà été dit, un *règlement* adopté par le Conseil et le Parlement européens est *d'application directe***.** Il ne devrait donc pas être nécessaire, en théorie, de le transposer dans les législations nationales, comme on le fait pour une directive. En fait, le RGPD contient deux catégories de dispositions : certaines se substituent complètement aux règles des Etats membres, par exemple en accordant directement des garanties aux personnes dont les droits ont été méconnus par un système de traitement des données[12]. Mais sur d'autres points, le texte est un peu comme une directive, il laisse aux Etats membres la possibilité de conférer des droits ou d'imposer des obligations aux personnes ou bien encore de prévoir des procédures, en complétant ainsi le RGPD. C'est ce que l'on appelle les « *marges de manœuvre nationales* » laissées aux Etats membres.

Ces marges de manœuvres nationales ont pu susciter des inquiétudes, notamment en Allemagne. En effet, si chaque Etat membre cherche à utiliser largement ces marges de manœuvre, l'objectif d'harmonisation du RGPD risque de ne pas être atteint.

Il en résulte qu'en France la *loi Informatique et libertés* de 1978, telle qu'elle a été moult fois modifiée par rapport à sa première mouture, notamment pour tenir compte des diverses directives européennes en matière de traitement des données, est restée théoriquement en vigueur. Mais, en fait, une loi nouvelle a dû tout de même être adoptée par le parlement français pour la mettre en conformité avec le nouveau RGPD : il s'agit de la **loi n° 2018-493 du 20 juin 2018,** promulguée le 21 juin 2018, dite loi **CNIL 3**, qui vient donc

---

éléments sont essentiels lors de la mise en œuvre de textes obligatoires et à effet direct. Le Règlement (CE) n° 864/2007 du Parlement Européen et du Conseil du 11 juillet 2007 sur la loi applicable aux obligations non contractuelles (Rome II) illustre parfaitement les difficultés qui peuvent en résulter. Il convient donc de saluer les éclaircissements apportés en ce domaine par un arrêt de la Cour de justice du 17 novembre 2011 (CJUE, 17 nov. 2011, Deo Antoine Homawoo contre GMF Assurances SA, C-412/10)

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

rapprocher la loi française de la lettre du RGPD tout en exerçant certaines « *marges de manœuvre nationales* ».

Toutefois, la complexité résultant de la combinaison du règlement européen et de la loi nationale n'a pas été complètement réglée avec la modification de la loi de 1978 par la loi du 20 juin 2018, tant et si bien que cette dernière loi a habilité le gouvernement [13] à prendre dans un délai de six mois une ordonnance, sur la base de l'article 38 de la constitution, afin de réécrire l'ensemble de l'ensemble de la loi de 1978 (Informatique et Libertés) dans le but, je cite : « *d'apporter les corrections formelles et les adaptations nécessaires à la* ***simplification*** *et à la* ***cohérence*** *ainsi qu'à la* ***simplicité de la mise en œuvre*** *par les personnes concernées des dispositions qui mettent le droit national en conformité avec le RGPD* ». Une ordonnance n° 2018-1125 a donc été prise le 12 décembre 2018, (publiée le 13 décembre 2018). Il s'agit d'une réécriture complète de la loi, puisque l'ordonnance a abrogé 72 articles de la loi de 1978, pourtant déjà modifiée en juin 2018. On observera qu'en réalité, l'**apport de l'ordonnance porte plus sur la forme que sur le fond :** le but est d'apporter des corrections formelles et adaptations nécessaires pour une meilleure articulation des textes et une meilleure lisibilité[14].

Il est prévu que les dispositions de l'ordonnance du 12 décembre 2018 entreront en vigueur au plus tard le 1er juin 2019 [15].

---

[13] en son article 32

[14] L'objectif affiché n'a cependant pas totalement été atteint. Le système des renvois, parfois en chaîne, utilisé dans l'ordonnance rend certains articles de la Loi Informatique et Libertés difficilement compréhensibles, ce qu'avait déjà souligné la CNIL dans son avis : c'est particulièrement le cas de certaines dispositions relatives aux données de santé, tel que l'article 65 de la loi issue de l'ordonnance.

[15] Exactement, l'ordonnance en même temps que le décret modifiant le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dans sa rédaction résultant de la présente ordonnance, et au plus tard le 1er juin 2019 et **au plus tard le 1er juin 2019.** Par ailleurs, un projet de loi de ratification de l'ordonnance devra être déposé dans les 6 mois à compter de sa publication de l'ordonnance.

Nous sommes donc à ce jour dans une période transitoire. Dans l'attente, les dispositions actuelles de la Loi Informatique et Libertés, dans sa version modifiée par la loi du 20 juin 2018, restent seules applicables…

Précisons que toutes ces règles nationales, contenues donc dans la loi de 1978 moult modifiée, ont vocation à s'appliquer dès lors que la personne concernée réside en France, y compris lorsque le responsable du traitement n'est pas établi en France.

Nous sommes ainsi dans une situation où, en cas de conflit entre la loi nationale et le règlement européen, le juge appliquera en priorité la loi interne, c'est à dire la loi de 1978 modifiée par la loi du 20 juin 2018 ou par l'ordonnance du 12 décembre 2018, qui joue ainsi le rôle d'une « loi-écran » entre le droit européen et la réglementation française. Toutefois, les requérants ou les requérantes peuvent toujours exiger l'application directe du règlement européen et soulever la contrariété éventuelle de cette loi par rapport à la règle européenne, ce qui déclenchera la procédure de contrôle de la conformité de la loi en cause par rapport au règlement européen, selon la procédure française dite de contrôle de conventionalité initiée par la jurisprudence du Conseil d'Etat *Nicolo* [16] avec une éventuelle question préjudicielle posée à la Cour de justice de l'Union européenne sur l'interprétation du RGPD.

Tels sont les textes que le juge français doit appliquer.

II LE JUGE DANS LE CADRE DU RGPD

Le RGPD concerne le juge :

1° Le RGPD définit une autorité de contrôle

2° Le RGPD définit des voies de recours juridictionnels

3° Le RGPD s'applique à l'activité même du juge

[16] 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.*

1° Le RGPD définit une autorité de contrôle

Le RGPD s'est efforcé de redéfinir le rôle des autorités de protection des données des pays membres. Dans son article 51, le RGPD dit que chaque Etat membre « *prévoit* ***qu'une ou plusieurs autorités publiques indépendantes sont chargées de surveiller l'application du présent règlement…*** *afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement et de faciliter le libre flux des données à caractère personnel au sein de l'Union* **». Le RGPD insiste en outre sur la nécessité de l'indépendance de cette autorité de contrôle.**

En application du RGPD, la loi française du 20 juin 2018, modifiant la loi du 6 janvier 1978, est venue naturellement désigner la **COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES (CNIL)**, créée par la loi du 6 janvier 1978 comme l'autorité de contrôle nationale.

L'Italie, pays centralisé comme la France, encore qu'à un degré moindre, a adopté la même solution [17] d'une autorité unique : Il **Garante per la protezione dei dati personali** è un'autorità amministrativa indipendente istituita dalla cosiddetta legge sulla privacy (**legge 31 dicembre 1996, n. 675**), poi disciplinata dal Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003 n. 196), come modificato dal Decreto legislativo 10 agosto 2018, n. 101. [18]

En Allemagne, par contre, en raison de la structure fédérale, il y a au total 18 autorités de contrôle qui sont indépendamment chargées du contrôle du droit de la protection des données. Il s'agit tout d'abord du **Bundesbeauftragte für den Datenschutz** [19], compétent

---

[17] I compiti del Garante sono definiti dal **Regolamento (UE) 2016/679** e dal **Codice in materia di protezione dei dati personali** (decreto legislativo 30 giugno 2003, n. 196), adeguato alle disposizioni del Regolamento (UE) 2016/679 tramite il **Decreto legislativo 10 agosto 2018, n. 101**, oltre che da vari altri atti normativi italiani e internazionali.

[18] Quest'ultimo ha confermato che il Garante è l'autorità di controllo designata anche ai fini dell'attuazione del Regolamento generale sulla protezione dei dati personali (UE) 2016/679 (art. 51). Il Garante per la protezione dei dati personali è un organo collegiale, composto da quattro membri eletti dal Parlamento, i quali rimangono in carica per un mandato di sette anni non rinnovabile. L´attuale Collegio è stato eletto dal Parlamento (ai sensi dell´art. 153, comma 2 del Codice) il 6 giugno 2012 e si è insediato 19 giugno 2012.* -

[19] commissaire fédéral à la protection des données

en particulier pour le respect de la protection des données personnelles par les autorités publiques fédérales. En outre, chaque Land dispose également d'une autorité chargée de superviser les entreprises situées sur son territoire ainsi que les autorités administratives. [20]

Pour en revenir à la France, l'adoption du RGPD entraîne une redéfinition et même un élargissement des pouvoirs de la CNIL. Sur ce point, je me limiterai à mettre en évidence deux aspects :

Premier aspect de l'évolution des pouvoirs de la CNIL : 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 délivrait la CNIL ont été supprimées[21].

Second aspect de l'évolution des pouvoirs de la CNIL : Dans le cadre du RGPD, la CNIL a vu son domaine d'activité accru, et notamment ses pouvoirs de sanction renforcés, avec la possibilité d'infliger des **amendes administratives très importantes[22]**. En cas de violation du règlement, ces amendes sont susceptibles désormais, selon le règlement, d'atteindre, en fonction de 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

[20] Le Land de Bavière constitue une particularité. Deux autorités indépendantes - une pour le secteur public et l'autre pour secteur privé - sont compétentes pour le contrôle de la protection des données

[21] 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 ceux qui intéressent **la sûreté de l'Etat, la défense ou la sécurité publique** 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 ;

[22] L'article 83 du RGPD prévoit de façon assez précise les conditions relatives à ces amendes

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 détermination de ces sanctions est laissée par le règlement à l'appréciation des Etats (c'est un exemple de « marge de manœuvre nationale »).

L'actualité la plus récente me permet d'illustrer ce pouvoir de sanction de l'autorité unique :

En Allemagne, très récemment une sanction liée au manquement en matière du règlement général sur la protection des données personnelles est tombée. Le site de réseau social Knuddels.de a en effet écopé d'une pénalité, d'un montant relativement peu important **au regard du maximum possible (20 millions d'euros ou 4% du chiffre d'affaires**), de 20 000 euros. **Cette dernière a été infligée dans le** Land voisin de Baden-Württemberg par le «LFDI», *Landesbauftragter fur Datenschutz und Informationsfreiheit* [23].

C'est la première mesure du genre outre-Rhin.

Et la commission nationale informatique et libertés, pour sa part, vient de prononcer contre Google, en application du RGPD, une amende record de 50 millions d'euros pour ne pas avoir suffisamment informé ses utilisateurs sur l'exploitation de leurs données personnelles. La plainte collective avait été déposée par les associations None Of Your Business et la Quadrature du Net. La CNIL devient ainsi la première instance de régulation européenne à sanctionner une grande plate forme numérique mondiale (*source https://www.le monde.fr/2019/01/21*).

2° Le RGPD définit des voies de recours juridictionnels

Le RGPD contient des dispositions sur les voies de recours [24] et en particulier, sur les voies de recours juridictionnels.

[23] Cette annonce intervient 4 mois après la révélation du leak en juillet dernier de près de 808 000 adresses mails et de plus d'1,8 million de noms d'utilisateurs et de mots de passe de ce site de chat en ligne. L'amende relativement modeste s'explique par le fait que l'autorité du Bade-Wurtemberg a pris en compte la transparence et la collaboration ainsi que la rapidité à implémenter les mises à jour de sécurité de Knuddels.

[24] Dans son chapitre VIII, en ses articles 77 à 82,

Le RGPD consacre notamment le droit à un recours juridictionnel *effectif*. En ce qui concerne la nature des recours juridictionnels, le règlement distingue les recours juridictionnels contre une autorité de cont-rôle (article 78) et les recours juridictionnels contre un responsable du traitement ou un sous-traitant (article79).

Le système existant en France lors de l'entrée en vigueur du RGPD peut être considéré comme répondant largement aux exigences d'un **recours effectif**, du moins du point de vue des recours devant le juge administratif. L'architecture générale classique de ces recours, recours pour excès de pouvoir, recours de pleine juridiction, complétée depuis l'introduction de procédures de référé telles que créées par la **loi** du 30 juin **2000**, référé suspension, référé-liberté, référé mesures utiles, répond en grande partie aux exigences de recours *effectif*. Il faut aussi préciser que les différentes modifications apportées à la loi informatique et libertés du 6 janvier 1978, en raison de la nécessité de tenir compte des directives européennes intervenues en la matière dès avant l'adoption du RGPD, avaient modifié ou précisé l'architecture générale des voies de recours en vue d'accroitre l'effectivité des voies de recours : Je pense notamment à la création par la loi n° 2004-801 du 6 août 2004 d'une procédure de sanctions à l'égard du responsable d'un traitement. Cette loi a notamment donné au président de la CNIL la place d'un requérant privilégié, en cas d'atteinte grave et immédiate aux droits et libertés en matière d'informatique pour 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 ces droits et libertés, disposition qui figure aujourd'hui à l'article 46 IV de la loi du 6 janvier 1978 modifiée pour assurer la sauvegarde des droits consacrés par le RGPD.

Les **recours juridictionnels contre l'autorité de contrôle** vont être organisés en France contre la CNIL. Dans notre droit interne, le juge administratif normalement compétent à l'égard des décisions de la CNIL est le CONSEIL D'ETAT, juridiction administrative suprême, ou pour reprendre l'expression usitée, « *juge ultime de l'administration* ». Le code de justice administrative dit en son article R.311-1 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). Le **contentieux de la CNIL est ainsi, pour la plus grande partie, centralisé devant le Conseil**

d'Etat, qui contrôle l'action de la CNIL, autorité unique nationale. Système qui donne au juge administratif un rôle central dans le contentieux du RGPD.

En Italie, le contentieux des décisions prises par l'autorité de contrôle (**Garante per la protezione dei dati personali),** dans un système où la répartition des compétences entre juridiction administrative et juridiction civile est fondé sur la distinction droits subjectifs/intérêt légitime, est confiée au juge ordinaire, à savoir le tribunal civil où réside le responsable du traitement des données. Au niveau du contrôle juridictionnel, il s'agit donc d'un système où le contentieux est décentralisé.

En Allemagne, tant que des amendes pécuniaires ne sont pas en jeu, les voies de recours du droit administratif sont ouvertes contre les mesures prises par les autorités de contrôle dans les Länder [25]

Pour la France, on observera que les décisions prises par la CNIL peuvent, comme toutes les autres décisions prises par des autorités administratives, 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 français.

A ce sujet, il faut constater l'ampleur de l'activité de la CNIL, telle qu'elle résulte désormais de l'application du RGPD : la CNIL donne des avis, établit des directives ou recommandations ou référentiels, des règlements types, reçoit des réclamations, fait procéder à des vérifications, certifie des données, etc et je le rappelle, inflige des sanctions. Il appartient donc au Conseil d'Etat de dire si ces actes sont susceptibles ou non de recours devant la juridiction administrative [26] :

[25] Cf Die Rolle der Aufsichtsbehörden nach der DSGVO, Vortrag in der Saarbrücken Tagung

[26] **Cf 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. En fait, il ne s'agissait pas d'une décision de la CNIL, qui s'était bornée en l'espèce à *notifie*r une décision du ministre de l'intérieur.

En tout cas, l'accroissement des compétences de la CNIL, pouvoir d'infliger des sanctions administratives et des amendes d'un montant élevé, tout cela pourrait être la source d'un accroissement du contentieux de la CNIL devant le Conseil d'Etat [27].

Pour les **recours juridictionnels contre un responsable d'un traitement** (ou un sous-traitant), qui aurait porté atteinte aux données personnelles par le responsable d'un traitement, le RGPD a consacré plusieurs types d'action juridictionnelle : Pour certaines, la loi interne française en avait déjà consacré l'existence (cf l'action de groupe), pour d'autres il a fallu les introduire dans la loi (cf recours en matière de transfert des données vers un pays tiers.

Pour ce qui est de l'action de groupe, elle est prévue par l'article 80 du RGPD [28]. Est visée ainsi une procédure de poursuite collective qui permet 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. Précisons que ces actions de groupe peuvent donner au lieu à des actions devant les juridictions administratives ou judiciaires.

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.

En fait, l'action de groupe a été introduite en France dès 2014, dans le domaine de la consommation [29], et elle a fait l'objet d'une **loi n° 2016-1547 du 18 novembre 2016, dite de modernisation de la justice du XXIe 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 et de qualité pour agir.

Cette loi de 2016, qui a entrainé une modification du code de justice administrative, a été adoptée après l'édiction du RGPD, mais avant son entrée en vigueur, ce qui fait que le code de justice administrative a défini, sur la base de la loi de 2016, avec un grand luxe de détails, la portée des actions de groupe en général et aussi en particulier des actions

[27] : la CNIL a déjà enregistré plus de 1 200 violations de données personnelles

[28] Le RGPD parle d''un 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* ».

[29] loi n° 2014-344 du 17 mars 2014 relative à la consommation,

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).

Aussi, pour tenir compte du RGPD, la loi du 18 novembre 2016 a dû être modifiée par la loi du 20 juin 2018 : Le manquement **par un responsable de traitement de données à caractère personnel** devient expressément le manquement aux obligations du RGPD. Il est précisé dans la loi que l'action peut être exercée soit en vue de faire cesser le manquement, soit en vue d'engager la responsabilité de la personne ayant causé le dommage afin d'obtenir la réparation des préjudices matériels et moraux subis, soit de ces deux fins.[30]

On voit que la législation française sur l'action de groupe est venue se couler naturellement et concomitamment au RGPD.

La suspension d'un transfert de données personnelles vers un pays tiers est au contraire une procédure nouvelle en droit français, imposée par l'entrée en vigueur du RGPD. Cette procédure est destinée à permettre à la CNIL de demander au Conseil **d'Etat la suspension d'un transfert de données personnelles** vers un pays tiers à l'Union européenne (ou à une organisation internationale). L'article 45 du RGPD prévoit en effet dans ce cas une *décision d'adéquation* de la Commission européenne, qui constate que le pays tiers en cause (ou l'organisation internationale) assure un niveau de protection adéquat. En conséquence, la loi française du 20 juin 2018 [31] est venue conférer la possibilité à la CNIL, la Commission nationale de l'informatique et des libertés donc, lorsqu'elle est saisie d'une réclamation par une personne intéressée qui estime que ses droits et libertés sont violés par un transfert de données, de demander au Conseil d'Etat d'ordonner la suspension de ce transfert. La compétence du Conseil d'Etat est justifiée ici par le fait que la légalité d'une décision de la commission européenne est en jeu. La

---

[30] Le code de justice administrative modifié précise bien que 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. On a bien ici un recours de pleine juridiction.

[31] Article 43 quinquies de la loi du 6 janvier 1978, modifiée par la loi du 20 juin 2018

particularité de la procédure ainsi organisée est que la loi prévoit l'obligation pour la CNIL, lorsqu'elle introduit ce recours, de demander au Conseil d'Etat **de poser une question préjudicielle à la Cour de justice de l'Union européenne** en vue d'apprécier la validité de la décision de la Commission européenne prise sur le fondement de l'article 45 du RGPD. Il y a là l'introduction d'une voie de recours tout à fait particulière dans le droit français, dont le champ d'application est large, que le transfert de données soit le fait d'une personne publique ou privée.

On pourrait encore mentionner les procédures suivantes :

Le mandat à une association pour agir devant la Commission nationale de l'informatique et des libertés ou devant un juge contre le responsable de traitement (ou même contre ladite commission) lorsqu'est en cause un traitement de données à caractère personnel en matière pénale par une autorité publique [32].

Le sursis à statuer (introduit pas l'article 81 du RGPD[33]) pour une juridiction d'un Etat membre 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.

3° L'application du RGPD à l'activité juridictionnelle :

Ici, je me bornerai à évoquer le fait que, dans le cadre des « marges de manœuvre nationales », la loi du 20 juin 2018 précise, en son article 10, « *qu'aucune décision de justice*

[32] ARTICLE 43 quater de la loi de 1978 version juin 2018 ou 38 (version juin 2019).

[33] 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.

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 »**.**

Dans cette optique, l'anonymisation des décisions de justice contenues dans les banques de données devant la juridiction administrative française, qui est en pratique depuis quelques années déjà, va dans le sens du RGPD.

III APERÇU DE JURISPRUDENCE

Il n'y a pas à ce jour, à ma connaissance, de décisions des juridictions administratives, en matière d'application du RGPE. Seul le conseil constitutionnel s'est prononcé lors de l'entrée en vigueur de la loi du 20 juin 2018. Mais quelques décisions du Conseil d'Etat précédant l'entrée en vigueur du RGPD peuvent avoir ouvert des pistes pour la jurisprudence future ;

- **La décision du Conseil constitutionnel français n° 2018-765 DC du 12 juin 2018**. Dans le cadre du contrôle de constitutionnalité *a priori,* des sénateurs ont déféré au Conseil constitutionnel la loi du 20 juin 2018, en dénonçant son inintelligibilité et en soutenant que le texte méconnaissait l'objectif de valeur constitutionnelle d'accessibilité et d'intelligibilité de la loi compte tenu des divergences entre les dispositions de la loi du 6 janvier 1978, telle que modifiée, et le règlement européen du 27 avril 2016. Selon eux, cette absence de 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 et validé dans ses grandes lignes la loi.

:

- L'action de la CNIL contre le ministre de l'intérieur du 9 mars 2018 : la CNIL, en tant que personnalité chargée de s'assurer du contrôle de la liste noire, agissant donc en tant que requérante, 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 d'Etat 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. En fait, il ne s'agissait pas d'une véritable décision de la CNIL, qui s'était bornée en l'espèce à notifier une décision du 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.

CONCLUSIONLe sujet combine la complexité de l'informatique et du droit ! L'impression qui peut être dominante est la complexité des textes, tant au niveau de leur contenu que de l'articulation entre le droit national et le droit européen. Cela peut entraîner des difficultés et des interrogations pour le juriste, certes.

Mais à l'heure où l'on voit apparaître un sentiment antieuropéen grandissant, on assiste avec l'introduction d'un règlement au niveau européen (rappelons qu'aux Etats Unis, il n'y a pas actuellement de législation fédérale globale sur la protection des données personnelles), lequel entend assurer la protection des données personnelles des personnes physiques, tout en laissant aux Etats membres, dans le respect de leur organisation constitutionnelle et judiciaire, des marges de liberté (marges de manœuvre nationale) (où sont les diktats de Bruxelles ?). Dans cette architecture générale, le rôle du juge, et dans le cas français, le rôle du juge administratif, est consacré et développé en vue d'assurer une meilleure protection des droits et libertés. L'Europe, ça ne fonctionne pas si mal.