Protection des données à caractère personnel et régime transnational

Degrave, Elise

Published in:
Traité de droit administratif européen

Publication date:
2022

Document Version
le PDF de l'éditeur

CHAPITRE II.
Protection des données à caractère personnel et régime transnational

Elise DEGRAVE[1]

INTRODUCTION

Nul ne l'ignore, les outils numériques ont envahi la vie quotidienne, dans tous les domaines. Leur efficacité se nourrit notamment de l'utilisation massive des données à caractère personnel des citoyens. Au-delà de l'indéniable enthousiasme suscité par ces technologies émergent maintes questions liées, entre autres, à la protection de la vie privée de chacun. C'est pourquoi, aujourd'hui, le défi majeur en cette matière est d'organiser un juste équilibre entre, d'une part, la circulation des données, préalable nécessaire à l'efficacité technologique, et, d'autre part, la protection des droits et libertés des citoyens, fondement de nos sociétés démocratiques et élément essentiel du libre épanouissement de chacun. Pour y parvenir, il importe d'encadrer subtilement et de contrôler effectivement les traitements de données à caractère personnel effectués par les responsables de traitement, qu'il s'agisse des États, des sociétés privées ou des individus. Ce défi est d'autant plus grand que les traitements de données revêtent de plus en plus souvent un caractère transnational.

Pour clarifier d'emblée les termes cardinaux de la matière, précisons qu'un « traitement » vise toute utilisation des données à caractère personnel des individus, qu'il s'agisse de leur collecte, leur enregistrement dans une base de données, leur mise à disposition sur un site internet, la transmission de celles-ci par courriel, etc. La notion de « donnée à caractère personnel » est également très large puisqu'il s'agit de toute information relative à une personne physique identifiée ou identifiable, telle qu'un nom et un prénom mais aussi un numéro de compte bancaire, un numéro de plaque d'immatriculation, une adresse mail, une adresse IP permettant de localiser un ordinateur, etc.[2]

(1) Professeure à la Faculté de droit de l'Université de Namur ; directrice de recherches au Namur Digital Institute (NADI) et au Centre de recherches Information droit et société (Crids) co-directrice de la Chaire Egov. Le texte est à jour au 1er avril 2019.

(2) Dans la suite de cette étude, nous parlerons de « données » pour viser les « données à caractère personnel ».

L'ensemble des innombrables traitements de données constitue l'une des matières premières de ce que nous appelons ici le secteur du numérique. Celui-ci présente des particularités intéressantes pour l'étude du droit administratif européen.

En effet, le secteur du numérique est *intangible et transfrontière*. Les données, immatérielles, sont aussi ubiquitaires. Quand bien même elles seraient stockées dans une base de données localisée sur le territoire d'un État précis, elles peuvent être consultées, copiées, envoyées, enregistrées à de multiples endroits dans le monde, en quelques « clics ». Le constat n'est pas différent lorsque les données figurent sur un site internet potentiellement consultable par tous. Il est donc fréquent qu'au final, plusieurs États soient concernés par l'utilisation de mêmes données. Il en va d'autant plus ainsi que dans ce secteur émergent nombre d'entreprises multinationales, notamment les GAFAM[3], dont l'activité s'étend sur l'ensemble du territoire européen et même bien au-delà. Quelles sont alors les règles à appliquer ? De quelles autorités, administratives ou juridictionnelles, relève leur contrôle ? « Le fait que l'architecture technique d'Internet ait été élaborée sans tenir compte du découpage territorial entre les États déstabilise le système traditionnel [...] de l'égalité souveraine des États et de non-ingérence dans les affaires intérieures »[4], si bien qu'aujourd'hui, « la grande difficulté liée à l'avènement du numérique réside dans la transposition à cet univers des règles d'organisation spatiale qui ont été pensées dans le monde analogique »[5]. On comprend d'emblée combien cette situation peut ébranler le droit administratif, fondé sur le principe de territorialité.

Intangible et transfrontière, le secteur du numérique est également marqué par la *rapidité* et la *technicité* des questions à réguler. Ce secteur étant étroitement lié au développement des technologies, les aspects à encadrer revêtent un côté technique, complexe, bien souvent abstrait. C'est aussi un domaine particulièrement mouvant, qui évolue très rapidement. Dès lors, pour ce qui est des règles qui encadrent les traitements de données, on ne peut exiger du législateur qu'il les définisse seul, et, *a priori*, « une fois pour toutes ». Le législateur a besoin d'être relayé, sur le terrain, par des autorités administratives indépendantes, appelées « autorités de contrôle », qui ont à leur disposition des moyens d'action plus souples et plus rapides. Nous y reviendrons.

S'agissant du cadre juridique de la matière, en droit de l'Union européenne, la protection des données fait partie du droit primaire. L'article 16 TFUE

(3) Google, Apple, Facebook, Amazon et Microsoft.

(4) C. de Clercq et F. Dechamps, « Internet à l'épreuve du droit ou le droit à l'épreuve d'Internet. Une analyse au regard de la problématique de l'étendue géographique du droit européen au déréférencement », *J.T.*, 2017, p. 670.

(5) V.-L. Benabou, « La Cour de justice, gardienne d'une "souveraineté européenne" sur les données personnelles », *R.A.E-L.E.A.*, 2018, p. 24.

et l'article 8 de la Charte des droits fondamentaux de l'Union européenne consacrent le droit de chacun à la protection des données à caractère personnel qui le concernent. Chacune de ces dispositions confie le respect des règles de protection des données au contrôle d'autorités indépendantes.

Au niveau du droit dérivé, la directive 95/46[6] a longtemps constitué l'assise de la protection des données au sein de l'Union européenne. Ce texte fixait le cadre de la matière, tout en laissant aux États une large marge de manœuvre. Cela a certes favorisé la mise en place de règles et d'organes dédiés à la protection des données des citoyens européens, mais il en a résulté des disparités nombreuses entre les règles et pratiques de chaque État. Ce fut le cas au niveau des autorités de contrôle nationales[7]. La directive a rendu ces autorités obligatoires, tout en laissant aux États membres le soin d'en définir les contours, ce qui a provoqué des différences parfois importantes dans le statut et les pouvoirs d'action de ces institutions.

Depuis, la protection des données des citoyens européens a pris un tournant nouveau avec l'adoption du RGPD[8], entré en application le 25 mai 2018. Ce texte constitue une évolution (et non une révolution) de la matière, rendue nécessaire par le déploiement important d'Internet et des outils numériques depuis une vingtaine d'années.

Entre autres évolutions, le RGPD renforce le rôle des autorités de contrôle en les dotant de pouvoirs plus nombreux et plus précis et introduit des règles spécifiques relatives à leur indépendance. En outre, le RGPD organise la coopération transfrontière entre les autorités de contrôle, ce qui nous intéresse tout particulièrement dans le cadre de cette étude.

Cette étude se concentre sur le rôle et le statut de l'autorité de contrôle, avant d'aborder sur les traitements de données transfrontaliers, lesquels impliquent une coopération entre les autorités de contrôle sous l'égide du Comité européen de la protection des données.

(6) Dir. 95/46 du Parlement européen et du Conseil du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

(7) Agence des droits fondamentaux de l'Union européenne (FRA), *La protection des données à caractère personnel dans l'Union européenne : le rôle des autorités nationales chargées de la protection des données. Renforcement de l'architecture des droits fondamentaux au sein de l'UE II*, 2012, accessible ici : http://fra.europa.eu/fr/publication/2012/la-protection-des-donnes-caractre-personnel-dans-lunion-europenne-le-rle-des.

(8) Règl. (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 96/46/CE.

Section I. Autorité de contrôle : son rôle et son statut

1. **Une autorité incontournable.** « Chaque État membre prévoit qu'une ou plusieurs autorités publiques indépendantes sont chargées de surveiller l'application du présent règlement, afin de protéger les libertés et les 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 (ci-après dénommée "autorité de contrôle") ».

C'est en ces termes que le RGPD, en son article 51, impose à chaque État membre l'obligation de mettre en place une autorité administrative spécifiquement dédiée au contrôle des traitements de données à caractère personnel. Le rôle de l'autorité de contrôle est si important que le RGPD y consacre un chapitre entier, le chapitre VI, intitulé « Autorités de contrôle indépendantes ». En effet, le RGPD, comme d'ailleurs la directive 95/46 avant lui, érige l'autorité de contrôle en « élément essentiel de la protection des données »[9]. Et pour cause. Le régime juridique de la protection des données risquerait bien de n'être qu'un vœu pieux sans une autorité chargée de faire connaître ces règles et de veiller à leur application dans la pratique.

D'emblée il apparaît que les autorités de contrôle ont un statut particulier. Il s'agit d'autorités publiques, organisées selon le droit national, qui agissent conformément au droit administratif national. Mais leurs tâches sont imposées par le droit de l'Union européenne. Leurs missions et leurs prérogatives étaient définies assez largement sous l'égide de la directive 95/46. Elles ont été considérablement précisées par le RGPD, ce qui laisse désormais peu de marge de manœuvre aux législateurs nationaux[10].

Historiquement, les premières autorités de contrôle sont apparues très tôt, dès les années 1970, à l'occasion des réflexions entourant l'informatisation de l'administration et l'apparition des craintes liées à l'utilisation des données à caractère personnel des citoyens dans un État informatisé. Ces autorités étaient alors conçues comme les « chiens de garde » des premières bases de données étatiques, chargés d'en baliser l'accès et d'empêcher l'usage abusif des données qui y étaient enregistrées. Ainsi, par exemple, en France, ces peurs sont nées avec le projet SAFARI[11]. Il s'agissait, pour l'État, d'attribuer à chaque citoyen un numéro d'identification unique pour tous les fichiers publics, de manière à faciliter le regroupement de leurs informations. Les vives contestations rencon-

(9) Consid. 62 de la dir. 95/46 ; consid. 117 RGPD.

(10) Pour une analyse des dispositions du RGPD laissant une marge de manœuvre aux législateurs nationaux, voy. H. Hijmans, « The DPAs and Their Cooperation: How Far Are We in Making Enforcement of Data Protection Law More European? », *EDPL*, 2016, pp. 364 et s.

(11) SAFARI est l'acronyme de « système automatisé pour les fichiers administratifs et le répertoire des individus ».

trées par ce projet ont abouti à l'adoption de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et à l'institution de la Commission nationale de l'informatique et des libertés (CNIL). Quelques années plus tard, en Belgique, c'est un même émoi qui a été suscité par la création du Registre national en 1983, première base de données étatique regroupant les données d'identification de chaque citoyen belge. La Commission consultative de la protection de la vie privée a alors été créée pour rendre des avis relatifs à l'accès au Registre national et à l'utilisation du numéro d'identification au Registre national. Depuis lors, cette Commission a évolué pour devenir la Commission de la protection de la vie privée, aujourd'hui remplacée par l'Autorité de protection des données depuis l'entrée en application du RGPD.

Des années plus tard, en 1995, la directive 95/46 a imposé à chaque État la mise en place d'une autorité de contrôle. Néanmoins, ainsi qu'on l'a dit plus haut, la marge de manœuvre laissée aux législateurs nationaux était importante, si bien que de nombreuses disparités sont apparues dans le statut et les compétences de chacune de ces autorités.

Aujourd'hui, le RGPD impose non seulement l'existence de ces autorités, mais aussi des critères précis quant au statut et aux compétences de celles-ci, en intégrant notamment la jurisprudence de la Cour de justice de l'Union européenne[12] relative à l'indépendance de l'autorité de contrôle[13].

2. **Le rôle de l'autorité de contrôle.** L'autorité de contrôle est un corégulateur, un conseiller et un contrôleur[14].

En tant que *corégulateur*, l'autorité de contrôle est un relais utile du législateur au niveau de la définition des règles de protection des données. Ainsi, par exemple, il revient à l'autorité de contrôle d'établir et de publier une liste des types de traitements de données pour lesquels une analyse d'impact relative à la protection des données est requise[15].

Elle est aussi un *conseiller*, dans la mise en œuvre de la matière. Entre autres tâches, elle sensibilise les responsables du traitement en ce qui concerne les obligations qui leur incombent[16], elle aide le public à comprendre ses droits par

(12) Ci-après « CJUE ».

(13) Au sujet de cette jurisprudence, voy. E. Degrave, « Titre 11. L'autorité de contrôle », in C. de Terwangne et K. Rosier (dir.), *Le Règlement général sur la protection des données (RGPD/GDPR)*, coll. Crids, Bruxelles, Larcier, 2018, pp. 599-601.

(14) Dans le même sens, V. Verbruggen, « Titre 1. RGPD : cœur du puzzle de l'encadrement de la protection des données à caractère personnel dans l'Union européenne », in C. de Terwangne et K. Rosier (dir.), *Le Règlement général sur la protection des données (RGPD/GDPR)*, *op. cit.*, p. 55. Pour une analyse détaillée du rôle de l'autorité de contrôle, voy. E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, coll. Crids, Bruxelles, Larcier, 2014, pp. 562 et s.

(15) Art. 35, §§ 4 et 57, § 1, k), RGPD.

(16) Art. 57, § 1, d), RGPD.

rapport aux traitements de données[17], etc. Pour ce faire, elle développe des formulaires, pour l'introduction de plaintes notamment, qui sont autant d'éléments participant « à la construction de la pratique de l'autorité de contrôle »[18].

Enfin, elle est un *contrôleur*, chargé de veiller au respect effectif de la protection des données. L'autorité de contrôle dispose de moyens juridiques classiques, tels que le fait de dénoncer une infraction aux autorités judiciaires. Mais sa capacité de réaction et d'intervention est renforcée grâce à des moyens d'action plus souples, et, dès lors, mieux adaptés que les moyens traditionnels au caractère technique et rapide du secteur du numérique. On songe notamment au rappel à l'ordre, à l'interdiction de continuer un traitement illégal ou à l'amende[19]. On peut voir là « un exemple d'abandon par le législateur des modes traditionnels de règlements des conflits »[20], voire un certain assouplissement du droit administratif en faveur d'une plus grande efficacité de l'action administrative dans le secteur du numérique. Cette particularité n'est sûrement pas sans lien avec le constat dressé par l'Agence européenne des droits fondamentaux (FRA) en 2014 : l'autorité de contrôle étant conçue comme une instance à laquelle toute personne peut s'adresser directement pour mettre en œuvre ses droits, « les autorités de protection des données se sont révélées être la voie à suivre la plus populaire – et bien souvent la seule voie pertinente – pour les personnes demandant réparation dans les cas de violations de la protection des données »[21].

3. **Le statut de l'autorité de contrôle.** Une autorité de contrôle forte doit être indépendante des responsables du traitement qu'elle contrôle. C'est ce qu'a rappelé la Cour de justice de l'Union européenne dans trois arrêts qui interprètent l'exigence d'indépendance des autorités de contrôle et dont le RGPD s'est nourri pour circonscrire cette exigence.

L'exigence d'indépendance, telle qu'imposée par le RGPD, vise les membres de l'autorité de contrôle. Ceux-ci « demeurent libres de toute influence extérieure »[22] et « s'abstiennent de tout acte incompatible avec leurs fonctions »[23], notamment. Cette indépendance vise aussi l'institution elle-même, qui

(17) Art. 57, § 1, b), RGPD.

(18) V. Verbruggen, « Titre 1. RGPD : cœur du puzzle de l'encadrement de la protection des données à caractère personnel dans l'Union européenne », *op. cit.*, p. 56.

(19) Art. 58 RGPD.

(20) F. Rigaux, « Chapitre 3. Les paradoxes de la protection de la vie privée », in *Rapport n° 1 sur Internet et la vie privée*, p. 39, disponible à l'adresse www.asmp.fr/travaux/gpw/internetvieprivee/rapport1/chapitr3.pdf (dernière consultation : 14 janvier 2019).

(21) Agence européenne des droits fondamentaux (FRA), « Accès aux voies de recours en matière de protection des données à caractère personnel dans les États membres de l'UE », 2014, p. 5, https://fra.europa.eu/fr/publication/2014/accs-aux-voies-de-recours-en-matire-de-protection-des-donnes-caractre-personnel.

(22) Art. 52, § 2, RGPD.

(23) Art. 52, § 3, RGPD.

doit, par exemple, disposer « des ressources humaines, techniques et financières [...] nécessaires à l'exercice effectif de ses missions et de ses pouvoirs, y compris lorsqu'elle doit agir dans le cadre de l'assistance mutuelle, de la coopération [...] »[24]. Par ailleurs, l'autorité de contrôle « dispose de ses propres agents [...] »[25] et « dispose d'un budget annuel public propre [...] »[26].

Cette indépendance vaut par rapport à toute influence extérieure, y compris celle des institutions européennes. C'est pourquoi, lors des discussions préalables à l'adoption du RGPD, l'indépendance de l'autorité de contrôle a été invoquée[27] pour faire supprimer une disposition figurant dans la proposition initiale de la Commission[28]. Dans le souci d'assurer une application harmonieuse des règles de protection des données partout dans l'Union européenne, cette disposition habilitait la Commission à adopter « une décision motivée enjoignant à l'autorité de contrôle de suspendre l'adoption du projet de mesure » lorsque « la Commission nourrit des doutes sérieux quant à savoir si le projet de mesure permet de garantir la bonne application du présent règlement » et ce, dans le cadre du mécanisme de contrôle de la cohérence, qui vise les traitements de données concernant des personnes établies dans différents États membres[29]. Il a été soutenu que « le modèle proposé par la Commission ne garantit toutefois pas la nécessaire indépendance des autorités de protection des données »[30]. Pour cette raison, cette disposition ne figure pas dans la version finale du RGPD.

(24) Art. 52, § 4, RGPD.

(25) Art. 52, § 5, RGPD.

(26) Art. 52, § 6, RGPD.

(27) Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen, rapport de J.P. Albrecht sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) (COM[2012] 0011-C7-0025/2012-2012/0011[COD]), 21 novembre 2013, A7-0402/2013, p. 226.

(28) Commission européenne, Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), COM(2012) 11 final, 2012/001 (COD), 25 janvier 2012.

(29) Voy. *infra*.

(30) Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen, rapport de J.P. Albrecht, *op. cit.*, p. 226 ; amendement 169 mentionné dans la Résolution législative du Parlement européen du 12 mars 2014 sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) (COM[2012] 0011-C7-0025/2012-2012/0011[COD]), *JO*, C 378/472, 9 novembre 2017. Dans le même sens, voy. Groupe de travail « Article 29 », avis 01/2012 du 23 mars 2012, sur les propositions de réforme de la protection des données, WP 191, pp. 22 et 23.

Section II. Traitements de données transfrontaliers au sein de l'UE : la coopération entre les autorités de contrôle sous l'égide du Comité européen de la protection des données

A. Un « traitement transfrontalier » et une « autorité chef de file »

4. **« Traitement transfrontalier ».** À la faveur du déploiement des multinationales, il n'est pas rare qu'une entreprise qui traite des données à caractère personnel[31] ou qui sous-traite celles-ci[32] soit établie dans plusieurs États membres. Un traitement de données qui a lieu dans le cadre de l'activité de ces établissements est un « traitement transfrontalier », au sens de l'article 4, 23), du RGPD[33].

> *Par exemple, une entreprise de vente de vêtements en ligne a son siège à Berlin, en Allemagne, et est également établie dans plusieurs autres États membres. Tous ces établissements utilisent le même logiciel pour traiter les données à caractère personnel des consommateurs. Ces traitements de données sont des traitements transfrontaliers*[34].

> *Autre exemple, l'entreprise Google Europe a son siège à Dublin, en Irlande, et une trentaine d'établissements dans les autres États membres. Lorsque Google traite les données de l'ensemble des utilisateurs européens à des fins d'analyse comportementale et de ciblage publicitaire, il réalise des traitements de données transfrontaliers*[35].

5. **L'« autorité chef de file ».** Quelle est l'autorité de contrôle compétente pour contrôler pareil traitement de données transfrontalier ?

La directive 95/46 était silencieuse quant à cette question, se contentant d'affirmer que chaque autorité de contrôle était compétente sur le territoire

(31) Une entreprise qui détermine les finalités et les moyens d'un traitement de données est qualifiée de « responsable du traitement », conformément à l'art. 4, 7), RGPD.

(32) Il s'agit d'une entreprise qui traite des données pour le compte d'un responsable du traitement. Elle est qualifiée de « sous-traitant », conformément à l'art. 4, 8), RGPD.

(33) L'article 4, 23), RGPD vise également une autre hypothèse dans laquelle on assiste à un traitement transfrontalier. Toutefois, nous n'approfondissons pas cette notion au risque de déborder de l'objet de notre étude.

(34) Cet exemple est inspiré du document suivant : Groupe de travail « Article 29 » sur la protection des données, « Lignes directrices concernant la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'une sous-traitant », adoptées le 13 décembre 2016 et révisées et adoptées le 5 avril 2017, WP 244 rev. 01. À noter que ce Groupe de travail « Article 29 » est désormais remplacé par le Comité européen de la protection des données (voy. *infra*).

(35) CNIL, délibération de la formation restreinte n° SAN – 2019-001 du 21 janvier 2019, prononçant une sanction pécuniaire à l'encontre de la société Google LLC.

de l'État membre dont elle relève[36]. En pratique, les entreprises dont l'activité s'étendait dans plusieurs États membres de l'Union devaient donc se mettre en contact avec chaque autorité de contrôle de chaque État membre dans lequel elles étaient établies, ce qui était fastidieux.

Dans le souci d'alléger ces démarches administratives, le RGPD instaure le mécanisme dit « du guichet unique » (*one stop shop*). Désormais, en cas de traitement transfrontalier, une « autorité de contrôle chef de file » doit être désignée. Cette autorité de contrôle est celle du lieu de l'établissement principal du responsable du traitement, entendu comme l'établissement où sont prises « les décisions quant aux finalités et aux moyens du traitement de données à caractère personnel » et qui a « le pouvoir de faire appliquer ces décisions »[37]. Notons que ce mécanisme ne s'applique qu'aux entreprises. Les traitements effectués par des autorités publiques ou des organismes privés en exécution d'une obligation légale ou d'une mission d'intérêt public restent contrôlés exclusivement par l'autorité de contrôle de l'État membre concerné[38].

Ce mécanisme a soulevé des craintes et des discussions préalablement à l'adoption du RGPD.

Le citoyen, tout d'abord, risquait d'être éloigné du suivi de sa plainte, compte tenu du fait que l'autorité chef de file est celle de l'établissement principal de l'entreprise, et se situe peut-être à l'étranger. Comme l'a affirmé la CNIL, « cela signifie qu'en cas de problème pour un internaute sur un réseau social dont l'établissement principal est implanté dans un autre État membre, cette plainte sera traitée par l'autorité de ce dernier [...] », ce qui « renforcera l'image bureaucratique et lointaine des institutions communautaires »[39]. Craignant que ce mécanisme n'empêche le citoyen de voir sa demande instruite par l'autorité de contrôle qui lui est la plus proche et la plus accessible, d'aucuns ont réclamé le « maintien de la compétence de l'autorité de l'État membre de résidence du plaignant »[40].

D'autres craintes ont concerné les autorités de contrôle elles-mêmes. Une autorité de contrôle qui n'est pas l'autorité de contrôle chef de file peut tout de même se sentir concernée par le traitement transfrontalier en cause.

> C'est le cas, par exemple, lorsque le responsable du traitement est établi dans un État A, mais que des personnes établies dans un État B sont

(36) Art. 26.6 de la dir. 95/46.

(37) Art. 4, 16), RGPD.

(38) Art. 55.2 RGPD.

(39) CNIL, « Projet de règlement européen : la défense de la vie privée s'éloigne du citoyen », cnil.fr, 26 janvier 2012.

(40) Avis du Comité économique et social européen sur la « Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) », COM(2012) 11 final, 23 mai 2012, p. 96.

sensiblement affectées par une activité de traitement menée par le responsable du traitement. L'autorité de contrôle de l'État A souhaiterait légitimement avoir un regard sur la manière dont le dossier sera traité bien qu'elle ne soit pas l'autorité de contrôle chef de file.

Ériger en « chef de file » une seule des autorités de contrôle concernées par un traitement de données transfrontalier a fait naître la crainte que ce modèle conduise à « transformer les autres autorités de contrôle en de simples "boîtes aux lettres" »[41].

Or, malgré une volonté commune de protéger les données au sein de l'Union européenne et un socle commun de règles à ce sujet, chaque État membre poursuit les préoccupations et les valeurs qui lui sont chères, ce qui peut entraîner des divergences dans la manière d'interpréter les règles de protection des données et de gérer les dossiers en la matière. Par ailleurs, une autorité de contrôle fonctionne avec les moyens humains et financiers qu'elle reçoit de l'État membre dont elle relève. On ne peut exclure que certaines autorités aient, plus que d'autres, les moyens de mener à bien leurs actions de contrôle et de sanction. Dès lors, pour une autorité de contrôle, accepter que la gestion du dossier relève exclusivement d'une autre autorité de contrôle, c'est prendre le risque que le dossier ne soit pas géré comme elle aurait voulu et pu le faire, alors même que le problème initial concerne les citoyens de l'État membre dont elle relève. En d'autres termes, puisque les traitements de données transfrontaliers touchent aux droits fondamentaux de citoyens de plusieurs États membres, on peut raisonnablement penser qu'une autorité de contrôle, soucieuse de protéger les individus de l'État membre dont elle relève, ait des difficultés à laisser la gestion du dossier exclusivement à une autorité tierce.

La crainte que le mécanisme du guichet unique éloigne du dossier tant le citoyen que les autorités de contrôle qui ne sont pas chefs de file explique que ce mécanisme s'accompagne, d'une part, de l'implication dans le dossier de l'autorité de contrôle ayant été saisie par le plaignant et, d'autre part, de la mise en place d'un système de coopération renforcée entre les autorités de contrôle concernées.

B. Saisine de l'autorité de contrôle par le citoyen

6. **Le maintien de la proximité avec le citoyen.** Pour que le mécanisme du guichet unique n'éloigne pas le citoyen du suivi du dossier lorsque le

(41) Avis de la Commission des affaires juridiques à l'intention de la Commission des libertés civiles, de la justice et des affaires intérieures sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), COM(2012) 0011-C7-0025/2012-2012/0011(COD), 25 mars 2012.

responsable du traitement est établi à l'étranger, il importait qu'il puisse porter plainte auprès de l'autorité de contrôle de « son lieu de résidence habituelle »[42].

Désormais, l'article 77 du RGPD affirme, en substance, que « toute personne concernée a le droit d'introduire une réclamation auprès d'une autorité de contrôle, en particulier dans l'État membre dans lequel se trouve sa résidence habituelle, son lieu de travail ou le lieu où la violation aurait été commise, si elle considère que le traitement de données à caractère personnel la concernant constitue une violation du présent règlement » et que cette autorité de contrôle « informe l'auteur de la réclamation de l'état d'avancement et de l'issue de la réclamation ».

En pratique, ainsi que l'affirme la CNIL sur son site internet, « le guichet unique facilite [...] les démarches des entreprises concernées, sans pour autant impacter les personnes concernées par ces traitements : leur autorité de protection des données nationale reste leur seul interlocuteur. Les personnes résidant en France peuvent ainsi continuer à adresser leurs plaintes à la CNIL, même si celle-ci n'est pas l'autorité chef de file à l'égard de ce traitement »[43].

C. Coopération renforcée entre les autorités de contrôle concernées

7. **Éviter les « boîtes aux lettres ».** Ainsi qu'on l'a dit, les autorités de contrôle craignaient d'être réduites à des « boîtes aux lettres » à défaut d'être autorité chef de file. Il n'aurait donc pas été admissible d'organiser, par le mécanisme du guichet unique, la création d'actes transnationaux entendus comme « des actes émanant de la puissance publique et soumis au droit administratif, qui déploient leurs effets juridiques dans les autres États membres de l'Union européenne par détermination du droit de l'Union européenne »[44] sans impliquer, dans la décision finale du dossier, l'ensemble des autorités de contrôle concernées par le traitement de données transfrontalier litigieux.

Par ailleurs, il fallait également s'assurer que la cohérence dans l'application des règles européennes soit plus effective que sous l'égide de la directive 95/46, ce qui justifiait que soit organisée « une coopération étroite entre les autorités »[45]. Avant même que ne soit entamée la réforme des règles de protection

(42) Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen, rapport de J.P. Albrecht, *op. cit.*, p. 51, amendement 169.

(43) www.cnil.fr/fr/le-guichet-unique.

(44) M. Gautier, « Acte administratif transnational et droit de l'Union européenne », in J.-B. Auby et J. Dutheil de la Rochère (dir.), *Traité de droit administratif européen*, t. 2, Bruxelles, Bruylant, 2014, p. 1305.

(45) Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen, rapport de J.P. Albrecht sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère

des données européennes, la Commission avait d'ailleurs annoncé qu'elle s'intéresserait aux moyens de « garantir une application plus cohérente des règles de l'UE en matière de protection des données dans tout le marché intérieur, notamment en renforçant le rôle des contrôleurs nationaux de la protection des données, en coordonnant mieux leur action par l'intermédiaire du groupe de travail "Article 29" (qui devrait devenir un organe plus transparent), et/ou en créant un mécanisme destiné à assurer une cohérence dans le marché intérieur sous l'autorité de la Commission européenne »[46].

8. **La notion d'« autorité de contrôle concernée ».** Pour répondre à ces préoccupations, le RGPD consacre la notion d'« autorité de contrôle concernée ». Il s'agit des autorités de contrôle qui ont un lien avec un traitement de données transfrontalier, soit parce que le responsable du traitement est établi sur le même territoire que l'autorité de contrôle, soit parce que les citoyens d'un État membre sont sensiblement affectés par le traitement ou sont susceptibles de l'être, soit parce qu'une réclamation a été introduite auprès de cette autorité[47]. Chaque autorité de contrôle concernée doit être impliquée dans le mécanisme de coopération renforcée, ainsi qu'on l'explique ci-après.

D'autre part, la coopération entre l'autorité de contrôle chef de file et les autorités de contrôle concernées a été précisée et renforcée par rapport au texte initial de manière à ce que chaque autorité de contrôle soit réellement impliquée dans le contrôle du traitement de données transfrontalières. En outre, le Comité européen de la protection des données a été créé[48].

9. **Le mécanisme de coopération renforcée.** Ce mécanisme est encadré par les articles 56 et 60 du RGPD[49]. Désormais, lorsque le citoyen soumet à une autorité de contrôle une réclamation concernant un traitement transfrontalier, cette autorité prend contact avec l'autorité de contrôle de l'établissement principal du responsable du traitement. Cette autorité de contrôle devient l'autorité chef de file pour le contrôle du traitement transfrontalier concerné par la réclamation[50].

---

personnel et à la libre circulation de ces données (règlement général sur la protection des données) (COM[2012] 0011-C7-0025/2012-2012/0011[COD]), 21 novembre 2013, A7-0402/2013, p. 226.

(46) Commission européenne, « Une approche globale de la protection des données à caractère personnel dans l'Union européenne », 4 novembre 2010, COM(2010) 609 final, p. 20.

(47) Art. 4, 22), RGPD.

(48) Voy. *infra*.

(49) Le Groupe de travail « Article 29 » sur la protection des données, désormais remplacé par le Comité européen de la protection des données (voy. *infra*), a rédigé des « Lignes directrices concernant la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant », citées à la note 35. Ce document, très clair, envisage nombre d'hypothèses qui dépassent le cadre de cette étude. Nous y renvoyons le lecteur désireux d'approfondir le sujet, et notamment la notion d'« établissement principal » d'un responsable du traitement.

(50) Art. 56.2 RGPD.

Une fois cette autorité chef de file désignée, celle-ci devient responsable de la gestion du dossier. Toutefois, il importe qu'elle n'agisse pas seule de son côté. L'autorité de contrôle chef de file et les autorités de contrôle concernées doivent coopérer « dans le respect des points de vue de chacune d'entre elles, pour garantir que le cas est examiné et résolu à la satisfaction de chaque autorité »[51], selon les termes du Groupe de travail « Article 29 ».

Plus précisément, cela signifie qu'au stade du traitement du dossier, les autorités de contrôle se prêtent mutuellement assistance[52] (transmission d'informations utiles, mise en place de mesures pour coopérer efficacement, etc.). Elles peuvent également mener des opérations conjointes[53] (enquêtes conjointes, mesures répressives conjointes, etc.). Le Groupe de travail « Article 29 » recommande d'ailleurs que les autorités de contrôle « s'efforcent d'adopter une ligne de conduite mutuellement acceptable », concernant, par exemple, la manière dont les enquêtes sont menées.

Au moment de prendre la décision finale, chaque autorité de contrôle coopère également, en « s'efforçant de parvenir à un consensus », selon les termes de l'article 60, 1), RGPD. À cet égard, l'autorité de contrôle chef de file « communique, sans tarder, les informations utiles aux autres autorités de contrôle concernées »[54]. Ensuite, elle leur propose un projet de décision[55]. Si celui-ci ne suscite pas d'objections[56], l'autorité de contrôle chef de file adopte la décision, la notifie au responsable du traitement et informe notamment les autres autorités de contrôle concernées.

De toute évidence, le succès de la coopération entre les autorités de contrôle est tributaire de la volonté de l'autorité de contrôle chef de file de collaborer effectivement avec les autorités concernées. En effet, si les informations pertinentes dans le dossier ne sont pas transmises au fur et à mesure de la procédure, d'autres garanties du RGPD pourraient être bousculées.

On pense, par exemple, à la possibilité, pour les autorités de contrôle concernées, de formuler des objections pertinentes à propos du projet de décision finale. Cela suppose que l'autorité de contrôle chef de file ne transmette pas seulement ce projet, mais également l'ensemble des éléments pertinents dans le dossier, pour que les autorités de contrôle concernées puissent se forger une opinion éclairée et juste et décider, le cas échéant, de formuler des objections.

(51) Groupe de travail « Article 29 » sur la protection des données, « Lignes directrices concernant la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant », *op. cit.*, p. 11.

(52) Art. 61 RGPD.

(53) Art. 62 RGPD.

(54) Art. 60.3 RGPD.

(55) *Ibid.*

(56) Pour l'hypothèse où des objections sont soulevées, voy. *infra*.

On songe également au fait que l'autorité de contrôle auprès de laquelle la réclamation initiale a été introduite doit informer l'auteur de la réclamation de l'état d'avancement et de l'issue de celle-ci[57]. Elle ne sera à même de remplir cette obligation et, par là, de répondre au souci de maintenir une proximité avec le citoyen malgré le mécanisme du guichet unique qu'en étant tenue au courant de la procédure au gré de son avancement.

Un autre élément non négligeable pour l'effectivité de la coopération entre les autorités de contrôle est le financement de celles-ci. À cet égard, le groupe de l'« Article 29 » devenu aujourd'hui l'EDPB (European Data Protection Board/ Comité européen de la protection des données) avait recommandé à l'époque que le RGPD précise quel est le budget que doit allouer chaque État à ces autorités, suggérant notamment que le montant soit calculé « à partir d'une formule tenant compte de la population d'un État membre et de son PIB »[58]. Le RGPD est malheureusement demeuré très flou sur ce point.

Précisons enfin que d'autres éléments doivent encore être rencontrés pour faire de la coopération une réalité. Comme l'a souligné le groupe de l'« Article 29 », « la langue utilisée, les délais, la quantité et la nature des informations demandées ainsi que les moyens techniques, les formats et les procédures pour l'échange des informations constituent des questions qui, dans la pratique, sont vitales pour assurer une coopération efficace entre les autorités chargées de la protection des données et sont donc également au cœur du principe de "guichet unique" »[59].

10. **Le contenu et la nature de la décision de l'autorité de contrôle chef de file.** Ainsi donc, au terme du processus de coopération, la décision finale est adoptée par l'autorité de contrôle chef de file.

Au niveau de son *contenu*, cette décision peut imposer au responsable du traitement l'une des mesures correctrices visées par le RGPD[60], telles qu'un avertissement, un rappel à l'ordre, une interdiction de traitement, la suspension d'un flux de données, une amende administrative, etc. S'agissant de l'amende en particulier, elle est perçue par l'autorité de contrôle auteure de la décision. Son affectation ultérieure est déterminée par le droit national de chaque État membre.

Mais alors, en cas de traitement transfrontalier, faut-il en conclure que seule l'autorité de contrôle chef de file perçoit l'amende, alors que celle-ci est liée à un traitement qui nuit à des citoyens établis sur le territoire de plusieurs États ? À l'heure actuelle, rien, dans le RGPD, ne permet malheureusement d'affirmer

(57) Art. 77.2 RGPD.

(58) Groupe de travail « Article 29 », Avis 01/2012 sur les propositions de réforme de la protection des données, WP 191, p. 19.

(59) *Ibid.*, p. 22.

(60) Art. 58 RGPD.

le contraire. Cela signifie donc que l'amende imposée à un responsable du traitement du fait d'un traitement de données illégal mené dans plusieurs États membres ne pourra au final être perçue que par un seul des États membres concernés. Or, étant donné que certains responsables du traitement, comme les GAFAM, sont plus enclins à s'établir dans certains États plutôt que d'autres, souvent pour des raisons fiscales, il est à craindre que quelques États, tels que l'Irlande ou le Luxembourg, perçoivent l'ensemble des amendes liées aux traitements transfrontaliers illégaux.

Pour rééquilibrer la situation entre les États membres, il pourrait être judicieux qu'une répartition équitable de l'amende soit définie dans le projet de décision finale et soit approuvée par les autorités de contrôle concernées. Par ailleurs, l'on regrette que l'autorité de contrôle chef de file soit nécessairement l'autorité du lieu d'établissement principal du responsable du traitement. Il eût fallu, selon nous, laisser la possibilité de désigner comme chef de file l'autorité de contrôle qui reçoit la plainte introduite par un citoyen. De cette manière, une tournante aurait été assurée entre autorités de contrôle, chacune se répartissant l'amende à tour de rôle. Dans le même temps, la proximité avec le plaignant aurait été davantage organisée.

Quant à la *nature* de la décision, celle-ci est contraignante pour le responsable du traitement et pour le plaignant. Cela signifie que la solution dégagée dans la décision de l'autorité de contrôle chef de file s'impose pour l'ensemble du traitement transfrontalier mené dans les divers États membres concernés.

Cette décision n'est pas sans conséquence pour les autres autorités de contrôle concernées. En effet, lorsque aucune autorité de contrôle n'a formulé d'objection pertinente et motivée dans le délai requis[61], toutes les autorités de contrôle concernées sont réputées approuver cette décision et sont liées par elle[62]. En d'autres termes, les autres autorités de contrôle concernées sont dessaisies du pouvoir d'adopter une décision relative au même traitement transfrontalier.

11. **Le respect des droits des parties concernées (le plaignant et le responsable du traitement).** Comme l'affirme explicitement le RGPD, les autorités de contrôle sont soumises à la Charte des droits fondamentaux de l'Union européenne[63] et, notamment, au droit de toute personne à une bonne administration[64], qui est un principe général de droit dans la jurisprudence de la CJUE[65].

(61) Voy. *infra*.

(62) Art. 60.6 RGPD.

(63) Art. 58.4 RGPD ; art. 51, 1), de la Charte.

(64) Art. 41 de la Charte.

(65) Voy. le commentaire de l'article 41 et les références jurisprudentielles citées par l'Agence des droits fondamentaux de l'Union européenne, https://fra.europa.eu/fr/charterpedia/article/41-droit-une-bonne-administration.

C'est pourquoi la décision de l'autorité de contrôle chef de file doit être motivée.

En outre, encore selon la Charte, avant d'adopter la décision finale concernant un traitement de données transfrontalier, l'autorité de contrôle chef de file doit notamment respecter « le droit de toute personne d'être entendue avant qu'une mesure individuelle qui l'affecterait défavorablement ne soit prise à son encontre »[66]. Ainsi, par exemple, avant qu'une mesure correctrice ne soit infligée à un responsable du traitement, l'autorité de contrôle doit lui permettre de faire valoir ses arguments.

Le règlement d'ordre intérieur de l'autorité de contrôle encadre la procédure permettant à chaque partie de faire connaître son point de vue. Il n'est toutefois pas obligatoire d'organiser l'audition des parties concernées. La communication d'observations écrites peut suffire, car ni la Charte, ni la jurisprudence de la CJUE n'imposent une audition[67].

12. **Le contrôle des décisions de l'autorité de contrôle chef de file.** Comme l'affirme explicitement le RGPD[68], la décision juridiquement contraignante d'une autorité de contrôle est susceptible d'un recours juridictionnel effectif, qui peut être formé par toute personne physique ou morale concernée par cette décision. Cela signifie que tant le responsable du traitement que le plaignant pourront contester en justice la décision de l'autorité de contrôle chef de file.

Ce recours doit avoir lieu devant les juridictions de l'État membre sur le territoire duquel l'autorité de contrôle chef de file est établie[69]. En l'occurrence, il s'agira donc des juridictions de l'État membre sur le territoire duquel le responsable du traitement a son établissement principal.

Force est alors de constater que cette situation ne répond pas au souci de maintenir une proximité avec le plaignant dans la gestion du dossier et qu'à cet égard, les entreprises semblent avoir été privilégiées par rapport aux citoyens. En effet, dans l'hypothèse où un citoyen introduit, auprès de l'autorité de contrôle de son pays, une réclamation contre un traitement transfrontalier effectué par un responsable du traitement dont l'établissement principal est dans un autre État membre, c'est l'autorité de contrôle de cet État qui sera

(66) Article 41, 1., a), de la Charte.

(67) P. Craig, « Article 41: Right to good administration », in S. Peers, T. Hervey, J. Kenner et A. Ward (éds.), *The EU Charter of Fundamental Rights – A Commentary*, Munchen/Oxford/Baden-Baden, Beck, Hart, Nomos, 2014, pp. 1069 à 1098 ; F. Tulkens, « Article 41. Droit à une bonne administration », in F. Picod et S. Van Drooghenbroeck (dir.), *Charte des droits fondamentaux de l'Union européenne – Commentaire article par article*, Bruxelles, Bruylant, 2017, p. 884.

(68) Art. 78 RGPD. L'article 47 de la Charte est également applicable en vertu de l'article 58.4, précité.

(69) Art. 78.3 RGPD.

l'autorité de contrôle chef de file. Dès lors, si le citoyen souhaite attaquer la décision rendue par cette autorité, il devra le faire dans un État qui n'est pas le sien, mais bien celui de l'établissement principal du responsable du traitement.

Quant à la procédure à suivre pour effectuer ce recours, elle est déterminée par le droit national. À nouveau, dans l'hypothèse où un citoyen intente un recours contre la décision d'une autorité chef de file établie dans un autre État membre que le sien, cela peut représenter de lourdes contraintes supplémentaires, notamment pour prendre connaissance du droit local et, le cas échéant, surmonter des difficultés linguistiques.

13. **Résoudre les difficultés dans la coopération.** Le système qui vient d'être décrit fait fi des embûches éventuelles qui surviendraient dans le déroulement de la procédure. Or, on ne peut exclure que le processus de coopération entre les autorités de contrôle concernées ne se passe pas toujours de manière aussi fluide. Le RGPD a donc envisagé les hypothèses où cette coopération rencontrerait des difficultés, en attribuant un rôle clé au Comité européen de la protection des données.

D. Comité européen de la protection des données et mécanisme de contrôle de la cohérence

14. **Un nouvel acteur de la protection des données.** Pour assurer l'application cohérente des règles européennes de protection des données, le RGPD met en place le Comité européen de la protection des données (ci-après « EDPB » pour *European Data Protection Board*[70]).

L'EDPB est un nouvel organe de l'Union[71] dédié à la protection des données. Son rôle est de veiller à l'application cohérente du RGPD[72] sur le territoire de l'Union européenne. C'est un organe indépendant[73], doté de la personnalité juridique[74]. Cela signifie qu'il agit de manière autonome, tout en étant juridiquement responsable de ses actes.

L'EDPB remplace le Groupe de travail « Article 29 », qui œuvrait, par ses recommandations, à l'interprétation uniforme des règles de protection des données dans l'Union européenne. Désormais, c'est l'EDPB qui assurera ce rôle, notamment *via* la publication de lignes directrices, de recommandations

(70) Nous évitons l'acronyme « CEPD », déjà utilisé pour viser le contrôleur européen de protection des données, qui est l'autorité de contrôle chargée de veiller à ce que les institutions et les organes de l'Union européenne respectent le droit à la protection de la vie privée des citoyens lorsqu'ils traitent des données à caractère personnel (pour de plus amples précisions, voy. https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_fr).

(71) Art. 68.1 RGPD.

(72) Art. 70.1 RGPD.

(73) Art. 69 RGPD.

(74) Art. 68 RGPD.

et de bonnes pratiques « afin de favoriser l'application cohérente »[75] du RGPD. Il pourra ainsi guider l'interprétation des règles européennes, ce qui devrait favoriser la cohérence dans la mise en œuvre de la matière au sein de l'Union européenne. On s'en réjouit compte tenu du fait qu'en cette matière, de plus en plus de questions ont un caractère transnational.

Le rôle de l'EDPB va plus loin que celui du Groupe de travail « Article 29 ». En cela, il incarne une nouveauté dans l'univers de la protection des données. En effet, l'EDPB dispose d'un pouvoir de décision pour intervenir dans le mécanisme de contrôle de la cohérence, qui est un corollaire du mécanisme de coopération expliqué ci-dessus. À cet égard, il revient à l'EDPB d'assumer un rôle d'arbitre, en tranchant, *via* des décisions contraignantes, les litiges qui surviendraient entre autorités de contrôle amenées à coopérer à propos d'un traitement transfrontalier.

15. **Le mécanisme de contrôle de la cohérence.** Ainsi qu'on l'a évoqué, le mécanisme de coopération renforcée entre autorités de contrôle peut se heurter à des désaccords entre les autorités de contrôle concernées. Face à ces difficultés, l'EDPB sera appelé à exercer son rôle de garant de la cohérence, en tranchant le litige afin que la coopération puisse reprendre et ce, en vertu de l'article 65 RGPD consacré au « règlement des litiges par le comité ».

Trois cas de figure peuvent aboutir à l'adoption d'une décision contraignante de l'EDPB.

Dans le premier cas de figure, à l'entame du processus de coopération, les autorités de contrôle concernées ne s'accordent pas sur celle d'entre elles qui mérite la qualité d'autorité chef de file. Dans ce cas, il est important que l'EDPB puisse débloquer la situation en désignant l'autorité de contrôle chef de file qui mènera la suite du processus de coopération et à l'adoption de la décision finale.

Le deuxième cas de figure peut surgir à la fin du processus de coopération, lorsqu'une autorité de contrôle concernée formule une objection pertinente et motivée à l'égard du projet de décision proposé par l'autorité de contrôle chef de file. Si l'autorité de contrôle chef de file ne suit pas cette objection[76], l'EDPB peut être saisi pour trancher le litige.

Le troisième cas de figure ne concerne pas directement la coopération entre les autorités de contrôle. Il s'agit de l'hypothèse dans laquelle une autorité de

(75) Art. 70.1, e), RGPD.

(76) Remarquons qu'une erreur de traduction semble s'être glissée dans la version en français du RGPD, qui vise le cas où « une autorité de contrôle concernée a formulé une objection [...] *ou* que l'autorité chef de contrôle chef de file a rejeté cette objection » tandis que la version en anglais remplace le « ou » par un « et », ce qui nous semble plus cohérent.

contrôle ne demande pas l'avis préalable de l'EDPB alors qu'elle aurait dû le faire, en vertu de l'article 64.1 du RGPD[77].

16. **Le contenu et la nature des décisions de l'EDPB.** Au niveau du *contenu*, nous nous concentrons dans ces lignes sur les deux premiers cas de figure venant d'être énoncés.

Dans le premier cas, la décision de l'EDPB consiste à désigner l'autorité chef de file pour que le processus de coopération puisse commencer.

Le deuxième cas de figure suscite davantage de commentaires. Lorsqu'une autorité de contrôle a formulé une objection pertinente et motivée qui n'a pas été suivie par l'autorité de contrôle chef de file, il revient à l'EDPB de trancher le litige par une décision contraignante qui « concerne toutes les questions qui font l'objet de l'objection pertinente et motivée, notamment celle de savoir s'il y a violation du présent règlement »[78].

Doit-on comprendre que, dans ce cas, l'examen de l'EDPB est limité aux arguments soulevés dans l'objection et donc à la question de savoir si oui ou non cette objection doit être suivie ? Ou l'EDPB peut-il, à l'occasion du recours porté devant lui, soulever d'autres critiques relatives à la violation du RGPD ? En d'autres termes, imaginons que l'autorité de contrôle chef de file affirme qu'il n'y a pas eu violation de telle disposition du RGPD, alors qu'une autorité de contrôle concernée prétend le contraire. À l'occasion de l'examen du litige, l'EDPB découvre qu'une autre disposition du RGPD a été violée, sans que cela soit invoqué dans l'objection. L'EDPB doit-il se contenter de donner raison ou tort à l'autorité de contrôle concernée ou peut-il soulever lui-même l'argument non invoqué dans l'objection ?

Pour l'heure, l'EDPB n'a pas encore été saisi dans une procédure de ce type. Il n'est donc pas encore possible de commenter une quelconque jurisprudence. Néanmoins, à notre sens, la deuxième solution devrait prévaloir. Dès le moment où l'EDPB est saisi, il devrait pouvoir examiner tous les aspects du traitement transfrontalier en cause au regard de toutes les dispositions du RGPD. Cette interprétation nous semble donc nécessaire pour respecter l'essence même du rôle de l'EDPB, et la raison d'être de cet organe, à savoir celui de gardien du RGPD dans son ensemble[79]. Sans cela, l'EDPB pourrait bien n'être qu'un arbitre chargé d'apaiser les conflits entre autorités de contrôle.

(77) Nous n'approfondissons pas cette hypothèse qui s'éloigne de l'objet de notre étude.

(78) Art. 65.1, a), RGPD.

(79) Dans le même sens, voy. R. Robert, « Titre 12. Le Comité européen de la protection des données : le garant d'un nouvel ordre ? », in *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, *op. cit.*, pp. 632 et 633.

Quant à la *nature* des décisions de l'EDPB, celles-ci s'adressent à l'autorité de contrôle chef de file et aux autorités de contrôle concernées. Elles sont contraignantes à leur égard[80].

Il s'ensuit que la décision finale doit être adoptée par les autorités de contrôle concernées sur la base de la décision de l'EDPB, en faisant référence à cette décision qui doit être jointe à la décision finale[81].

Cela signifie que l'EDPB ne se substitue pas aux autorités de contrôle et ne prend pas lui-même la décision finale. Il effectue donc un contrôle de légalité, au regard du RGPD, de la décision finale contestée mais il doit ensuite renvoyer l'affaire à l'autorité de contrôle chef de file.

Ce constat est intéressant lorsqu'il s'agit, par exemple, d'imposer une amende à un responsable du traitement[82]. Il revient à l'EDPB de vérifier si une telle amende est justifiée et si, comme le requiert le RGPD[83], celle-ci est proportionnée, notamment. Mais les textes poussent à affirmer que c'est ensuite aux autorités de contrôle concernées de s'accorder sur le montant de celle-ci[84]. Cela paraît également opportun, vu que « l'autorité chef de file dispose d'une meilleure connaissance du dossier et pourra réévaluer le montant en suivant les procédures de sanction existant au niveau national »[85].

17. **Le respect des droits des parties concernées (le plaignant et le responsable du traitement).** En tant qu'organe de l'Union, l'EDPB est soumis au respect de la Charte des droits fondamentaux[86]. Tout comme les autorités de contrôle nationales, l'EDPB doit également respecter le principe de bonne administration, qui suppose notamment qu'il respecte « le droit de toute personne d'être entendue avant qu'une mesure individuelle qui l'affecterait défavorablement ne soit prise à son encontre »[87], ce qu'il peut faire par écrit[88]. Les règles de procédure de l'EDPB mentionnent ce droit explicitement[89].

À notre sens, tant le plaignant que le responsable du traitement bénéficient de ce droit. En effet, si l'EDPB venait à considérer que les arguments du plaignant ne sont pas fondés et que le traitement contesté ne justifie pas

(80) Art. 65.2 RGPD.
(81) Art. 65.6 RGPD.
(82) R. Robert, *op. cit.*, p. 633.
(83) Art. 83.1 RGPD.
(84) R. Robert, *op. cit.*, p. 633.
(85) *Ibid.*
(86) Art. 51 de la Charte.
(87) Art. 41, 1, a), de la Charte.
(88) Voy. *supra*.
(89) « *The Board shall make sure that all persons that might be adversely affected have been heard* ». Voy. art. 11.1 des règles de procédure de l'EDPB, adoptées le 25 mai 2018 et accessibles ici https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_rop2_adopted_23112018_en.pdf.pdf.

une sanction, cela pourrait affecter défavorablement le plaignant dans ce qu'il estime être une violation de ses droits fondamentaux. Il est important qu'au préalable, il ait pu faire valoir ses arguments. Il en va bien sûr de même pour le responsable du traitement si l'EDPB décidait de le sanctionner. C'est pourquoi l'EDPB devrait permettre aux deux parties de faire valoir leurs points de vue.

18. **Le contrôle des décisions de l'EDPB.** Les décisions du Comité sont qualifiables d'« actes [d'un] des organes de l'Union, destinés à produire des effets juridiques à l'égard des tiers »(90). Elles sont susceptibles d'être contrôlées par la Cour de justice par deux voies distinctes.

D'une part, en vertu de l'article 263 du Traité sur le fonctionnement de l'Union européenne, les décisions de l'EDPB peuvent faire l'objet d'un *recours en annulation* devant la Cour de justice de l'Union européenne, qui contrôlera la légalité de ces décisions.

Un tel recours peut être intenté par le responsable du traitement ou l'auteur de la réclamation, qu'il s'agisse d'une personne physique ou d'une personne morale. En effet, bien qu'ils ne soient pas les destinataires de la décision de l'EDPB, ils sont susceptibles d'être directement et individuellement concernés par cette décision et être de ce fait habilités à introduire ce recours(91). Le recours doit avoir lieu dans les deux mois de la publication de la décision sur le site internet de l'EDPB(92).

Le recours en annulation contre la décision de l'EDPB peut aussi être intenté, ce qui doit avoir lieu dans les autorités de contrôle concernées, qui sont les destinataires des décisions de l'EDPB. Le recours doit alors être intenté dans les deux mois de la notification qui leur a été faite de la décision(93).

Étant donné que la Cour est compétente pour se prononcer « sur les recours pour incompétence, violation des formes substantielles, violation des traités ou de toute règle de droit relative à leur application »(94), elle pourra se prononcer sur l'interprétation à donner au RGPD et, notamment, sur le caractère légal ou non des traitements contestés ainsi que le choix et l'ampleur des mesures correctrices à imposer dans chaque hypothèse.

D'autre part, en vertu de l'article 267 TFUE, une décision de l'EDPB peut également être soumise à l'examen de la Cour de justice *via* une question préjudicielle. Le considérant 143, alinéa 2, du RGPD détaille le contexte visé, qui est le suivant. Une autorité de contrôle a pris une décision pas moyen de changer le terme qui est juridique sur la base d'une décision de l'EDPB. La décision de

(90) Art. 263, al. 1, TFUE.
(91) Art. 263, al. 4, TFUE.
(92) Consid. 143 RGPD ; art. 263, dernier al., TFUE.
(93) *Ibid.*
(94) Art. 263, al. 2, TFUE.

cette autorité de contrôle est contestée devant une juridiction nationale. Dans le cadre de ce recours, la validité de la décision de l'EDPB est mise en cause. La juridiction nationale ne peut pas invalider elle-même la décision de l'EDPB. Dès lors, en principe, elle doit poser une question préjudicielle à la Cour de justice, relative à la validité de cette décision.

Néanmoins, il existe une exception à cette obligation. La juridiction nationale n'est pas obligée de poser la question préjudicielle demandée s'il s'avère que la personne physique ou morale concernée a eu l'occasion de former un recours en annulation contre la décision de l'EDPB mais ne l'a pas fait. Cela signifie que le responsable du traitement ou le plaignant doivent être très attentifs au délai de deux mois qui leur est imparti pour introduire un recours en annulation contre la décision de l'EDPB. Passé ce délai, ils ne pourront plus essayer d'obtenir que la Cour de justice invalide la décision du Comité par la voie d'une question préjudicielle(95).

Conclusion

Face à la multiplication des traitements de données effectués par des multinationales opérant au sein de l'Union européenne notamment, il était primordial de mettre en place de nouveaux mécanismes de coopération entre les autorités de contrôle et de renforcer l'harmonisation des règles applicables en Europe. La réforme opérée par le RGPD est donc la bienvenue.

En particulier, le souci d'alléger les charges administratives des entreprises et d'assurer une application cohérente des règles de protection des données partout dans l'Union européenne tout en veillant à maintenir la proximité du citoyen par rapport au suivi de son dossier de plainte a animé les discussions préalables au RGPD. Celles-ci ont finalement abouti à la mise en place d'un mécanisme de guichet unique, tout en permettant au citoyen de porter plainte auprès de l'autorité de contrôle de son État et d'être tenu au courant de l'avancement du dossier par celle-ci. L'EDPB, nouvel organe dans le paysage européen de la protection des données, se voit, quant à lui, doté d'un rôle inédit, celui de garant de l'application uniforme du RGPD, qui pourrait s'avérer essentiel dans l'interprétation et la mise en œuvre des règles de protection des données.

Il est encore trop tôt pour évaluer si ces objectifs sont atteints, notamment parce que l'EDPB n'a pas encore été saisi d'un dossier dans lequel il pourrait jouer son rôle de gardien de la cohérence.

Néanmoins, plusieurs éléments doivent retenir l'attention à ce stade.

(95) Voy. également R. Robert, *op. cit.*, p. 636.

S'agissant de l'objectif de proximité avec le citoyen malgré le mécanisme du guichet unique, il ne pourra être atteint que si l'autorité de contrôle chef de file joue pleinement le jeu de la collaboration, en informant régulièrement les autorités de contrôle concernées de l'avancement du dossier, de manière à ce que le plaignant soit ensuite tenu au courant de l'avancement du dossier par l'autorité de contrôle de son pays. Il apparaît toutefois que la proximité ne pourra de toute façon pas être atteinte s'agissant du recours qu'un plaignant souhaiterait intenter contre la décision finale de l'autorité de contrôle chef de file, puisque ce recours devra être intenté devant les juridictions de l'État où est établie cette autorité chef de file, s'accompagnant de toutes les difficultés de procédure et de langue que l'on devine.

Quant à l'harmonisation des règles de protection des données au sein de l'Union européenne, celle-ci se nourrira… ou pas… de l'attitude des autorités de contrôle et de l'EDPB. L'autorité de contrôle chef de file adoptera-t-elle plutôt une réaction de repli dans la gestion du dossier, ou saisira-t-elle l'opportunité offerte par le RGPD d'organiser notamment des opérations conjointes ? Quant aux autorités de contrôle concernées, auront-elles l'envie et les moyens de formuler des objections au projet de décision finale proposé par l'autorité chef de file, lorsqu'elles ne l'approuvent pas ? Et en cas d'objection, en quoi consistera le rôle de l'EDPB ? Assumera-t-il le rôle de gardien de la cohérence, par des interprétations et des décisions visant l'ensemble du RGPD, ou se contentera-t-il d'être un arbitre dans une procédure de résolution des litiges entre autorités de contrôle ?

Reste aussi la crainte que le contrôle du respect des règles de protection des données soit capturé par les autorités de contrôle des États dans lesquels s'établissent nombre d'entreprises, principalement pour des raisons fiscales. On pense à l'Irlande, sur le territoire de laquelle sont établis notamment Google et Facebook, ou au Luxembourg, où s'est établi Microsoft, entre autres. Outre la question de la collaboration se pose également celle de l'amende qui, à l'heure actuelle, n'est pas partagée entre les autorités de contrôle concernées.

On comprend donc combien les autorités de contrôle et l'EDPB sont appelées à jouer un rôle majeur dans la construction d'un régime juridique commun pour la protection des citoyens européens et dans l'effectivité de ces règles. Gageons du fait que ces institutions sauront se saisir au mieux des opportunités que leur offre le RGPD pour nourrir une collaboration constructive et efficace dans le contrôle des traitements de données transnationaux de plus en plus nombreux.

***

Annexe. Schéma récapitulatif du contrôle d'un traitement de données transfrontalier au sein de l'Union européenne